View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by Theseus

# Hämeen Monitoimitilien tietoliikenneratkaisujen ja -palveluiden kehittäminen


Ammattikorkeakoulun opinnäytetyö

Tietotekniikan koulutusohjelma

Riihimäen yksikkö kevät 2014

Jyri Lappalainen

HAMK
HÄMEEN AMMATTIKORKEAKOULU

TIIVISTELMÄ

Riihimäki
Tietotekniikka
Tietoliikennetekniikka

**Tekijä** Jyri Lappalainen **Vuosi** 2014

**Työn nimi** Hämeen Monitoimitilien tietoliikenneratkaisujen ja -palveluiden kehittäminen

TIIVISTELMÄ

Tässä opinnäytetyössä keskityttiin Hämeen Monitoimitilien tietoliikenneratkaisujen ja -palveluiden kehittämiseen. Opinnäyteyön toimeksiantaja oli Hämeen Monitoimitilit Oy. Hämeen Monitoimitilit on pieni tilitoimisto, jonka lähiverkkoa on hiljalleen laajennettu. Aluksi selvitettiin nykyisen tietoliikenneverkon toiminta, minkä jälkeen lähiverkosta laadittiin verkkokuva. Selvityksen jälkeen suunniteltiin lähiverkon kehitysideat. Lähiverkkoon tehtävillä muutoksilla pyrittiin parantamaan verkon toimintaa ja helpottamaan työntekoa.

Työn teoriaosassa perehdyttiin lähiverkon toimintaan ja siihen liittyviin laitteisiin ja tekniikoihin, sekä lähiverkon tietoliikenteeseen liittyviin tekniikoihin. Työssä tutkittiin myös lähiverkkojen kehittymistä lähitulevaisuudessa ja painopiste oli langattomissa palveluissa ja IPv6-protokollan tuomissa eduissa.

Lopputuloksena Hämeen Monitoimitilien lähiverkkoon toteutettiin tai suunniteltiin muutoksia, joiden avulla saatiin joustavampi ja paremmin toimiva lähiverkko. Lisäksi laadittiin katsaus lähiverkkojen mahdollistamiin palveluihin lähitulevaisuudessa ja lähitulevaisuuden kehitysnäkymistä, joiden avulla yrityksen lähiverkkoa voidaan kehittää jatkossa.

**Avainsanat** LAN, WLAN, IPv4, IPv6, Ethernet, Tietoverkot

**Sivut** 30 s. + liitteet 1 s.

HAMK
UNIVERSITY OF APPLIED SCIENCES

ABSTRACT

Riihimäki
Information Technology
Information Network Technology

**Author** Jyri Lappalainen **Year** 2014

**Subject of Bachelor's thesis** Development of IT-services in Hämeen Monitoimitilit

ABSTRACT

This thesis focuses on the development of IT-services in a company called Hämeen Monitoimitilit. The commissioner is a small accounting company that recently extended its local area network. The initial starting point was the defining of the present local area network and creating a network diagram. Development ideas were then planned based on this definition, with the purpose of making the network more functional and to facilitate working.

All related issues including functions of the local area networks, devices and techniques as well as data communications and its techniques are defined in the theoretical chapter. Development of the local area networks in the near future was researched with the focus on wireless services and IPv6.

As the final result, improvements were planned and executed in Hämeen Monitoimitilit's local area network , which clearly made the network more flexible and functional. An overview of the near future of local area networks and their development was also presented, so that the commissioner could take this into account when further developing their networks.

**Keywords** LAN, WLAN, IPv4, Ipv6, Ethernet, Network

**Pages** 30 p. + appendices 1 p.

SISÄLLYS

# Lyhenneluettelo

| | |
|---|---|
| ADSL | Asymmetric Digital Subscriber Line. Lankapuhelinlinjaa käyttävä digitaalinen tiedonsiirtotekniikka |
| CSMA/CD | Carrier Sense Multiple Access with Collision Detection. Tietoliikenteen siirtoväylän varausmenetelmä |
| DHCP | Dynamic Host Configuration Protocol. IP-osoitteiden jakopalvelu |
| DNS | Domain Name System. Internetin nimipalvelujärjestelmä, jonka tehtävä on muuttaa verkkotunnus IP-osoitteeksi. |
| ETHERNET | Pakettikytkentäisten lähiverkkojen yleisnimike |
| FTP | Foiled Twisted Pair. Foliosuojattu parikaapeli. |
| IEEE | Institute of Electronical and Electronics Engineers. Kansainvälinen tekniikan alan järjestö. |
| IP | Internet Protocol. Huolehtii datapakettien toimittamisesta perille Internetissä. |
| ISP | Internet Service Provider. Internet palvelun tarjoaja, ts. operaattorin verkko. |
| HTTP | Hypertext Transfer Protocol. Käytetään selaimissa ja WWW-palvelimissa tiedonsiirtoon. |
| LAN | Local Area Network. Maantieteellisesti rajoitettu tietoliikenneverkko, joka yhdistää alueen päätelaitteet toisiinsa. Tunnetaan yleisesti lähiverkkona. |
| MAN | Metropolitan Area Network. Alueverkko |
| MEDIA | Tiedonsiirtoväylä, esim. parikaapeli. |
| NAS | Network Attached Storage. Lähiverkon laite, useimmiten ulkoinen kovalevy, joka näkyy tallennusmediana verkon käyttäjille. |
| NAT | Network Address Traslation. Osoitteenmuunnos, jolla usea yksityisiä IP-osoitteita käyttävä päätelaite voi liikennöidä Internetissä yhdellä julkisella IP-osoitteella. |
| OSI-MALLI | Open Systems Interconnection Reference Model. Kuvaa tiedonsiirron protokollat kerrosmaisessa rakenteessa. |
| PAT | Port Address Translation. Porttimuunnos, joka mahdollistaa usean yhteyden yhdellä julkisella IP-osoitteella. |
| PoE | Power over Ethernet. Tekniikka, jolla voidaan siirtää virtaa parikaapelin avulla. |

| | |
|---|---|
| RDP | Remote Desktop Protocol. On Microsoftin kehittämä protokolla, jonka avulla voidaan luoda yhteys toiseen tietokoneeseen. |
| SMTP | Simple Mail Transfer Protocol. Käytetään viestien välittämiseen sähköpostipalvelimien välillä. |
| SSL VPN | Secure Sockets Layer Virtual Private Network on tekniikka, jossa otetaan VPN-yhteys SSL-yhteyden yli suljettuun verkkoon etätyöasemalta tai yhdistetään kaksi suljettua verkkoa keskenään. |
| STP | Shielded Twisted Pair. Suojattu parikaapeli, jossa jokainen pari on erillisen vaipan sisällä. |
| TCP | Transmission Control Protocol. Luo yhteyksiä päätelaitteiden välille, joilla on pääsy Internetiin. |
| UTP | Unshielded Twisted Pair. Suojaamaton parikaapeli. |
| VLAN | Virtual Local Area Network. Tekniikka, jolla fyysinen tietoverkko voidaan jakaa virtuaalisiin lähiverkkoihin loogisesti. |
| VoIP | Voice Over Internet Protocol. Tekniikka, jolla siirretään ääntä verkon yli reaaliaikaisesti. |
| VPN | Virtual Private Network. Yhteystapa, jolla muodostetaan suojattu yhteys julkisen tietoverkon läpi yrityksen verkkoon ja mahdollistaa täten etäyhteyden. |
| WAN | Wide Area Network. Laajaverkko |
| WLAN | Wireless Local Area Network. Tekniikka, jolla voidaan liittää päätelaitteita lähiverkkoon langattomasti. |

# 1 JOHDANTO

Tietoliikennepalvelut kehittyvät jatkuvasti ja kehitys on nopeaa. Yritysten lähiverkot, jotka yhdistävät yrityksen päätelaitteet, palvelut ja eri toimipisteet, ovat erityisen merkittävässä roolissa yritysten liiketoiminnan kannalta. Lähiverkot mahdollistavat nopean ja saumattoman tiedonsiirron ja parantavat täten yrityksen tehokkuutta. Tänä päivänä lähiverkon vaatimuksia otetaan huomioon jo rakennusvaiheessa tai yrityksen toimitilaa valittaessa ja monissa yrityksissä verkon suunnitteluun käytetään ulkopuolista apua.

Hämeen Monitoimitilit Oy on neljän hengen tilitoimisto, joka huolehtii asiakkaiden kirjanpidosta ja taloushallinnosta. Hämeen Monitoimitilien toimisto sijaitsee Riihimäellä, Hämeenaukiolla. Hämeen Monitoimitilien työntekijöillä ei ollut selkeää käsitystä heidän tämänhetkisistä tietoliikenneratkaisuistaan tai –palveluistaan, joten aiheen tutkiminen oli aiheellista. Lopullinen tavoite ja päämäärä on syventyä lähiverkon toimintaan ja siinä käytettyihin palveluihin ja tekniikoihin. Lähiverkkoa ja sen toimivuutta ja käytännöllisyyttä tutkittaessa pyrittiin parantamaan verkon toimivuutta ja poistamaan tai irtisanomaan mahdollisia turhia palveluita. Työn tarkoituksena on myös saattaa lähiverkko ajan tasalle ja laatia siitä selkeä verkkokuva. Pyrkimyksenä on myös laajentaa ja/tai muokata verkon palveluita asiakkaan toiveiden mukaisiksi, jotta heidän työntekoaan voitaisiin saada entistäkin helpommaksi ja tehokkaammaksi. Hämeen Monitoimitilien lähiverkko on osittain Elisan ja osittain Western Systemsin hallinnoima, joten muutoksien suhteen tehdään yhteistyötä näiden yritysten kanssa.

Työssä tutkitaan myös lähitulevaisuuden näkymiä ja kehityssuuntia lähiverkkojen osalta. Tulevaisuuden suuntaviivoja pyritään ottamaan huomioon myös Hämeen Monitoimitilien lähiverkon kehityksessä.

# 2 TYÖN RAJAUS JA MÄÄRITTELY

Tässä työssä perehdytään Hämeen Monitoimitilien lähiverkkoon. Aihetta lähestytään selvittämällä yrityksen lähiverkon tämänhetkinen tilanne. Lähiverkkoa tarkastellaan yleisesti käytössä olevien standardien ja käytäntöjen näkökulmasta. Tavoitteena on saada selkeä kuva tämänhetkisestä lähiverkosta ja pyrkiä kehittämään sitä yrityksen tarpeiden mukaan. Työssä pyritään selvittämään mahdollisuuksia parantaa yrityksen toimintaa kehittämällä lähiverkon tietoliikenneratkaisuja ja –palveluita.

Työn perustana on lähiverkko ja sen toiminnot. Lähiverkkoa ja sen rakennetta tutkitaan käyttäen hyödyksi Hämeen Monitoimitilien lähiverkkoa. Lähiverkosta käsitellään kaapelointia, verkkolaitteita ja erilaisia verkon tietoliikenteessä käytettyjä tekniikoita. Työ rajattiin vain yhden pienen yrityksen lähiverkkoon ja sen kehitystarpeisiin, jotta aihe pysyisi kasassa ja yhtenäisenä.

Työssä käsitellään myös lähitulevaisuuden lähiverkkojen kehittymistä ja sitä, kuinka se vaikuttaa yritysten tietoliikenneratkaisuihin ja yhteiskunnan

verkkoinfrastuktuuriin ja sen kehittämiseen tulevaisuuden tarpeiden mukaiseksi. Lähitulevaisuuden muutoksia on pyritty ottamaan huomioon myös Hämeen Monitoimitilien lähiverkon muutoksissa tarpeen mukaisesti.

# 3 LÄHIVERKKO

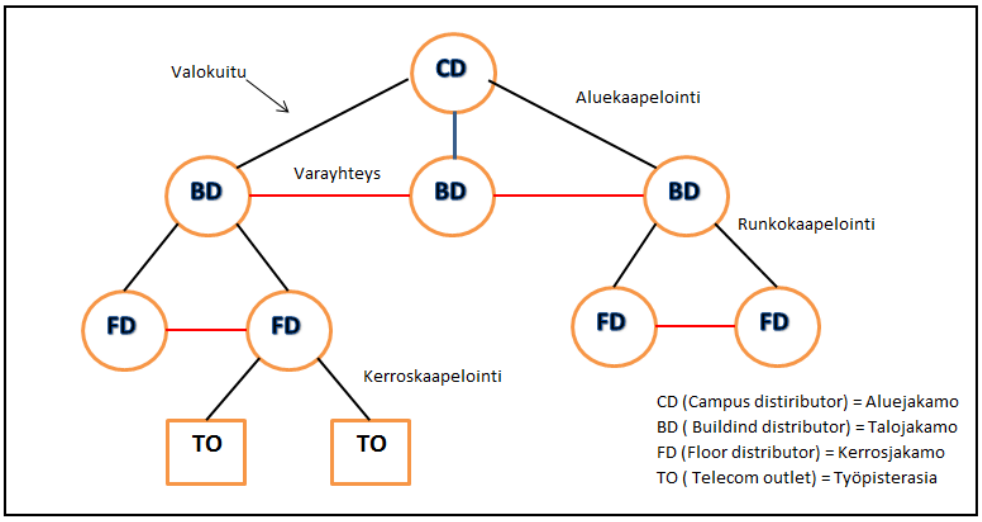
Lähiverkko eli LAN (Local Area Network) on maantieteellisesti rajattu ja tietyn alueen sisäistä tietoliikennettä toteuttava verkko, joka pystyy siirtämään suuria määriä dataa. Lähiverkot ovat yleisesti tietyn henkilön tai organisaation hallitsemia. Lähiverkko koostuu erilaisista laitteista, kuten reitittimistä, kytkimistä, palvelimista, työasemista ja kaapeleista. Lähiverkko voi myös olla osittain tai kokonaan langaton, jolloin puhutaan langattomasta lähiverkosta WLAN (Wireless LAN). Nykyisin yrityksien lähiverkot ovat usein osittain tai kokonaan jonkin ulkopuolisen tahon organisoimia, näin on myös Hämeen Monitoimitilien lähiverkon suhteen. Lähiverkkoja löytyy myös useimmista kotitalouksista, mutta ne sisältävät yleensä vain pienen määrän verkkolaitteita. Lähiverkkoja yhdistää nopea kaupunkialueen dataverkko, jota kutsutaan alueverkoksi MAN (Metropolitan Area Network). Tästäkin laajempaa tietoliikenneverkkoa kutsutaan termillä WAN (Wide Area Network), joka yhdistää maantieteellisesti suuria alueita yhteen ja näistä verkoista muodostuu eri maanosat yhdistävä maailmanlaajuinen tietoverkko. (Jaakohuhta, H. 2005, 4.)

## 3.1 Lähiverkon kaapelointi

Lähiverkko kuuluu nykyisin osana lähes jokaisen toimitilakiinteistön perustietoverkkoinfrastruktuuriin ja yleiskaapelointijärjestelmään. Nykyisin lähiverkon kaapelointi otetaan hyvin huomioon jo rakennusvaiheessa. Aiemmin yritysten lähiverkkojen luomiseen käytettiin puhelinkaapeleita, mutta tämä on jäämässä historiaan. Kaapeloinnilla yhdistetään verkon päätelaitteet, kuten työasemat, tulostimet ja palvelimet toisiinsa. Kaapeli toimii tiedonsiirtoväylänä verkkolaitteiden, päätelaitteiden ja verkossa toimivien palveluiden välillä. Lähiverkon kaapelointiin voidaan käyttää erilaisia standardoituja kaapeleita, joista yleisimmät ovat valokuitukaapelit sekä kierretyt parikaapelit. (Jaakohuhta, H. 2005, 35.)

### 3.1.1 Yleiskaapeloinnin rakenne

Yleiskaapeloinnissa tuodaan aluekaapelilla yhteys kiinteistön talojakamoon, josta yhteys viedään nousukaapeloinnilla kerroskohtaisiin kerrosjakamoihin. Useimmiten kerroskaapelointi toteutetaan kerrosjakamoista tähtimäisesti kaikille työpisterasioille. Yleiskaapelointiin liittyvät standardit on määritelty standardissa SFS-EN 50173. Standardi koskee kiinteistöjen tietoliikennekaapelointia. Kuvassa 1 on esitelty valokuidulla toteutettu kolmen erillisen rakennuksen lähiverkko. Hämeen Monitoimitileillä on kuitenkin käytössään ainoastaan yksi pieni toimipiste, joten erillisiä kerrosjakamoita ei tarvita, sillä laitemäärät ovat vähäisiä ja kaapelointietäisyydet ovat lyhyitä.




**Kuva 1. Yleiskaapeloinnin periaatekuva ( Jaakohuhta 2005, 53)**

### 3.1.2 Valokuitukaapelit

Valokuitu on ohutta muovista tai lasista valmistettua kuitua, joka johtaa valoa. Tietoliikenteessä sitä pitkin voidaan lähettää tietoa suurella nopeudella, jopa kymmeniä gigabittejä sekunnissa. Valokuitujen etuihin kuuluvat suuren tiedonsiirtokyvyn lisäksi mm. tietoturvallisuus, virheettömyys tiedonsiirrossa ja kaapelien helppo asennus ja käsittely. Haittapuolena on lasin herkkyys, minkä vuoksi valokuituja ei voi esimerkiksi taittaa jyrkästi. Valokuidut voidaan jaotella karkeasti kahteen ryhmään, yksimuotokuituihin ja monimuotokuituihin. (Teletekno 2006, 23-25.)

Yksimuotokuiduissa valo kulkee ytimessä heijastumatta suoraan päästä päähän. Yksimuotokuidut on valmistettu erittäin puhtaasta lasista. Yleisesti yksimuotokuituja käytetään tiedonsiirtoon pitkillä matkoilla. Optisten vahvistimien avulla voidaan toteuttaa kymmeniä kilometrejä pitkiä yhtämittaisia linkkejä. Esimerkiksi teleoperaattoreiden runkoverkot on rakennettu yksimuotokuiduilla. Yksimuotokuitua käytetään myös yleisesti rakennusten nousukaapeloinnissa.

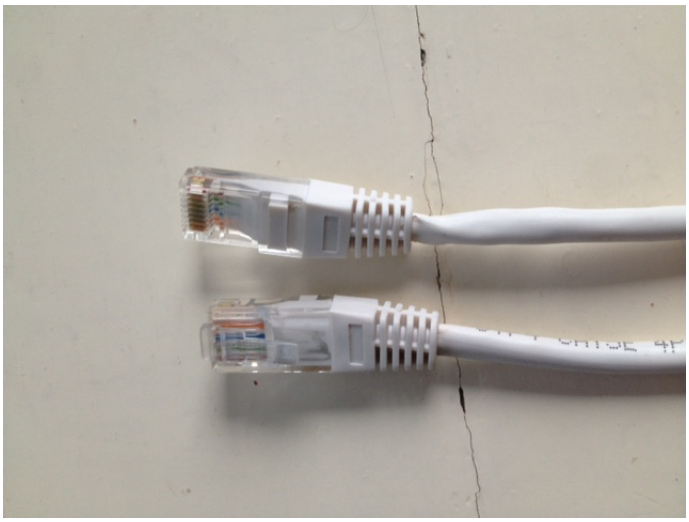
Monimuotokuiduissa valo kulkee heijastumalla ja taittumalla kuidun ytimen ja lasikuoren rajapinnasta. Monimuotokuituja voidaan valmistaa myös muovista ja niitä käytetään lyhyillä yhteysväleillä. Monimuotokuidut ovat selkeästi yksimuotokuituja edullisempia, mutta niillä ei pystytä muodostamaan kuin kymmenien tai satojen metrien mittaisia yhteyksiä, riippuen yhteyden nopeudesta. Monimuotokuitua voidaan yleisesti käyttää rakennusten sisäverkossa kerroskaapelointiin. Eri valokuitujen siirtonopeudet ja –pituudet on esitelty taulukossa 1.

Taulukko 1. Valokuitujen siirtonopeudet ja –pituudet

| Kategoria (ISO/IEC 11801) | Siirtonopeus | Suurin pituus |
|---|---|---|
| Yksimuotokuidut | | |
| OS1/OS2 | 10 Gb | 10 km |
| OS1/OS2 (vahvistimella) | 10 Gb | 40 km |
| OS1/OS2 | 40 Gb | 10 km |
| OS1/OS2 | 100 Gb | 10 km |
| Monimuotokuidut | | |
| OM1 | 100 Mb | 2000 m |
| OM1 | 1 Gb | 300 m |
| OM1 | 10 Gb | 30 m |
| OM2 | 10 Gb | 80 m |
| OM3 | 1 Gb | 1000 m |
| OM3 | 10 Gb | 300 m |
| OM3+ | 10 Gb | 550 m |
| OM3+ (OM4) | 40 Gb | 150 m |
| OM3+ (OM4) | 100 Gb | 150 m |

### 3.1.3 Parikaapelit

Kierretty parikaapeli on yleisin toimitiloissa käytetty kaapeli. Se on syrjäyttänyt koaksaalikaapeloinnin, jota enää harvoin käytetään lähiverkkojen kytkemiseen. Parikaapeli sisältää kaksi toistensa ympärille kierrettyä ja eristettyä johdinta, jotka on päällystetty muovilla. Johdinten kiertäminen toistensa ympärille vähentää sähköisiä häiriöitä johdossa kulkevaan signaaliin. Tiedonsiirtokapasiteetti kasvaa kaapelissa kulkevan taajuuden, eli kaistanleveyden kasvaessa. Kuvassa 2 on esitelty kierretty parikaapeli RJ-45 liittimillä, joka on yleisin parikaapeleissa käytetty liitintyyppi. (tlu.ee 2007.)



Kuva 2. Parikaapeli Cat5e RJ-45 liittimillä

Parikaapeleita on olemassa suojaamattomia ja suojattuja malleja. Suojaamattomissa kaapeleissa (UTP) parit on kierretty keskenään toisiinsa ja eroteltu omiin lohkoihin, jotka ovat ulkovaipan sisällä. Suojatuissa kaapeleissa (FTP) on tämän lisäksi erillinen metallivaippa ja erittäin hyvin suojatuissa kaapeleissa (STP) voi olla vielä lisäksi jokainen pari suojattuna erikseen. Kaapelin valinta riippuu paikasta, johon kaapeleita rakennetaan. Mitä enemmän ympäristö sisältää signaalia häiritseviä tekijöitä, kuten voimavirtakaapeleita, sitä paremmin sen tulee olla suojattu. Yleisimmin kuitenkin käytetään suojaamatonta kaapelia.

Parikaapelit on myös jaoteltu eri kategorioihin niiden ominaisuuksien mukaan. Parikaapelit on määritelty eri luokkiin, jotka on määritelty standardissa EN50173. Yleiskaapeloinnin erilaisten soveltuvuuksien vuoksi nykyisin vaaditaan vähintään kategorian 6 mukaista kaapelointia uusiin toimitiloihin. Hämeen Monitoimitilien sisäverkon kaapelointi on kategoriaa 5e, sillä rakennus on jo kymmeniä vuosia vanha, mutta uusiin toimistotaloihin ja muihin liiketiloihin on jo useamman vuoden ajan asennettu vähintään kategorian 6 mukainen kaapelointi. Tosin Hämeen Monitoimitilien tämänhetkiseen tiedonsiirtokapasiteetin tarpeeseen Cat5e-kaapelointi on riittävä. Tiedonsiirtokapasiteetin tarpeen kasvaessa, kehitetään jatkuvasti uusia ja parempia kaapeleita, joilla tietoa voidaan siirtää nopeammin ja enemmän. Kategorian 7a kaapeli on rakenteeltaan hyvin paljon kategorian 7 kaltainen, mutta kaistanleveyttä on kasvatettu ja kaapeliin on lisätty palmikkosuojaus. Kategoria 7a julkaistiin vuonna 2010. Suuremman kaistanleveyden ansiosta, kategorian 7a kaapelilla on onnistuttu testeissä siirtämään jopa 100 Gb/s, mutta vain hyvin lyhyitä matkoja ja yleisimmin sitä käytetään vain 10 Gb/s nopeudella. Kategorian 7a käyttö ei kuitenkaan ole kovin yleistä, verrattuna esimerkiksi kategorian 6 käyttöön. Kategorian 8 kaapeli on suunnitteilla Ethernet 40GB-T varten, mutta sitä ei ole vielä standardoitu. Kaapelien kategoriat ja suoritusarvot on esitelty taulukossa 2. (Ieee802.org 2013.)

Taulukko 2. Parikaapelien kategoriat ja suoritusarvot

| Kategoria | Siirtonopeus | Kaistaleveys |
|---|---|---|
| 5 | 100 Mb/s | 100 MHz |
| 5e | 1000 Mb/s | 100 MHz |
| 6 | 1000 Mb/s | 250 MHz |
| 6a | 10 Gb/s | 500 MHz |
| 7 | 10 Gb/s | 600 MHz |
| 7a | 10 Gb/s | 1000 MHz |
| 8 | 40 Gb/s | 1200 MHz |

## 3.2 Ethernet

Ethernet-verkko (IEEE 802.3) on eniten käytetty lähiverkkoratkaisu, jota käytetään suurimmassa osassa lähiverkoista. Se on väyläverkko, jonka toiminta perustuu kilpavaraukseen ja väylänvarausmenettelyyn. Ethernet-verkot käyttävät yhdenmukaisia kehyksiä, mikä mahdollistaa erilaisten protokollien ja medioiden käytön. Ethernetin juuret ovat jo 1970-luvulla, jolloin CSMA (Carrier Sense Multiple Access) todettiin toimivaksi väylänvarausmenettelyksi. Vuonna 1983, IEEE julkaisi suosituksen 802.3, joka tunnetaan myös nimellä IEEE 802.3 CSMA/CD. Tämän suosituksen pohjalta on nykyiset lähiverkot rakennettu. (Puska 2000, 45-47.)

### 3.2.1 Ethernet-ratkaisut

Ethernet on kehittynyt vuosien saatossa 10 Mb/s tiedonsiirtonopeudesta moninkertaiseksi. 100Base-verkkoja on lukuisia erilaisia, jotka poikkeavat ominaisuuksiltaan hieman toisistaan. Ylivoimaisesti eniten käytetty ratkaisu on kuitenkin 100Base-TX, joka on käytössä myös Hämeen Monitoimitilien lähiverkossa. Sen nimellinen tiedonsiirtonopeus on 100 Mb/s ja se tukee erittäin laajasti erilaisia medioita, standardeja ja laitteistoja. 100Base-TX edellyttää vähintään kategorian 5 kaapelointiluokkaa toimiakseen. (Granlund 2007, 284-285.)

Ethernet on kehittynyt jatkuvasti nopeammaksi. Vaikka 100Base-verkko onkin riittävä pieniin ja keskikokoisiin toimistoihin, kuten Hämeen Monitoimitileillä, ei senkään tiedonsiirtokapasiteetti välttämättä ole riittävä. Vuonna 1998 julkaistiin 1000Base, joka tunnetaan nimellä Gigabit Ethernet. Suorituskyky verrattuna edeltäjäänsä oli jälleen kymmenkertaistettu, mutta silti Gigabit Ethernet käyttää Ethernetistä tuttua väylänvarausmenetelmää ja kehystä. Gigabit Ethernet on tänä päivänä yleisesti käytetty ja tuettu eri valmistajien verkkolaitteissa. (Granlund 2007; Puska 2000.)

Ethernetistä on kehitetty myös 10GBase-ratkaisuja, joissa nopeus on jälleen kymmenkertaistettu. Suositus julkaistiin vuonna 2002. Verkko toimii ainoastaan kaksisuuntaisesti, eli full duplex -menetelmällä. 10 Gb/s tiedonsiirtonopeus mahdollistaa myös laajojen verkkojen toteuttamisen, joten

10GBase-ratkaisuja käytetään myös laajemmissa WAN-verkoissa. Ratkaisu mahdollistaa myös jopa 80 km:n pituiset välimatkat, joten se sopiikin hyvin runkoverkkojen toteuttamiseen. (Granlund 2007, 289.)

## 3.3 Langaton lähiverkko

Lähiverkkoja on käytetty jo vuosikymmeniä yhdistämään yritysten ja kotitalouksien verkkolaitteet toisiinsa. Nykyään nämä verkot voidaan toteuttaa myös langattomasti. Langattomista lähiverkoista käytetään termiä WLAN (Wireless Local Area Network). Tänä päivänä langattomat verkot vaikuttavat ihmisten jokapäiväiseen elämään. Langattomat verkot ovat mahdollistaneet sen, että ihmiset voivat olla verkossa lähes missä tahansa. Langattomia verkkoja löytyy mm. junista, kahviloista, kouluista yms. Monien liikkeiden ikkunasta voikin löytää Wi-Fi-merkinnän, joka kertoo, että tiloissa on käytettävissä ilmainen langaton internetyhteys. Langattomat lähiverkot ovat myös mahdollistaneet Internetin saatavuuden paikkoihin, joihin ei teleoperaattoreiden johtoja ole rakennettu. Langattomat lähiverkot mahdollistavat päätelaitteiden käytön ilman kaapelia, jolloin sisäverkon merkittävyys jää vähäisemmälle. Langattomuus lisää etenkin liikkuvuutta, mikä lisää vapautta ja helpottaa monissa elämäntilanteissa. Langattomia lähiverkkoja ja sen sovelluksia käytetäänkin nykyisin hyvin laajalla sektorilla ja mitä erilaisempien asioiden hoitamiseen. (Puska, M. 2005.)

IEEE 802.11 on IEEE:n standardi langattomille WLAN-lähiverkoille. Ensimmäinen WLAN-tekniikan standardi 802.11 julkaistiin vuonna 1997. Tekniikka on hyvin läheistä sukua Ethernetille (802.3). Tämän hetken suosituimmat IEEE 802.11 -sarjan standardit ovat 802.11a, 802.11g ja 802.11n. IEEE 802.11ac hyväksyttiin viralliseksi standardiksi vuoden 2014 alussa ja sen käyttö on kasvussa. Kehitteillä on myös standardi 802.11ad, joka ei vielä toistaiseksi ole laajasti käytössä. Taulukossa 3 on esitelty näiden standardien teoreettiset siirtonopeudet. (Perahia, E. Stacey, R. 2008, standards.ieee 2014.)

Taulukko 3. WLAN-standardien teoreettiset siirtonopeudet

| Standardi | Siirtonopeus |
|---|---|
| 802.11a | 54 Mb/s |
| 802.11g | 54 Mb/s |
| 802.11n | 600 Mb/s |
| 802.11ac | 1 Gb/s |
| 802.11ad | 7 Gb/s ? |

## 3.4 Kytkin

Kytkin (switch) yhdistää laitteita ja verkkoja toisiinsa välittämällä tiettyyn porttiin tulevan kehyksen mahdollisimman nopeasti siihen porttiin, josta löytyy kehyksen kohdeosoite. Kytkimet ovat nykypäivänä korvanneet vanhanaikaiset sillat ja keskittimet. Kytkimien oikeanlainen käyttö on erinomainen keino nopeuttaa lähiverkkoja ja tämän vuoksi kytkimet ovatkin nykyisten lähiverkkojen keskeisimpiä komponentteja. Kytkimen ideana on tarjota jokaiselle portille ja siihen kytketylle laitteelle Ethernet-verkon nimelliskaista. Kytkin tarkastaa myös kehyksen muotoa eli oikeellisuutta. Kehystä välittäessä on kytkimellä kolme vaihtoehtoa: välitys, tulvinta ja suodatus. Paketin saapuessa kytkimelle, kytkin tallentaa paketin lähettäjän MAC-osoitteen (Media Access Control) sekä portin, kytkimen osoitetauluun. Tämän jälkeen kytkin vertaa osoitetaulusta paketin vastaanottajan MAC-osoitetta ja sen löytyessä lähettää paketin eteenpäin oikean portin kautta oikeaan suuntaan. Tätä kutsutaan välitykseksi (forwarding). Mikäli vastaanottajan osoitetta ei ole taulussa, tai kyseessä on broadcast- tai multicast-paketti, lähettää kytkin paketin kaikkiin portteihin, paitsi siihen josta paketti on tullut. Tätä kutsutta tulvaksi (flooding). Jos vastaanottajan portti on sama kuin lähettäjän portti, paketti hävitetään. Tätä taas kutsutaan suodattamiseksi (filtering). Kytkimen porteissa voidaan myös käyttää erilaisia medioita, kuten valokuitua tai parikaapelia. Nykyisin olemassa olevia reitittäviä kytkimiä voidaan myös käyttää korvaamaan reitintä. (Jaakohuhta, H. 2005,137-150.)

## 3.5 Reititin

Reitittimen (Router) päätehtävänä on reitittää siihen saapuvat tietoliikennepaketit oikeisiin osoitteisiin. Reititintä käytetään eri verkkojen yhdistämiseen ja niiden välisten yhteyksien luomiseen. Reititintä voidaankin pitää tienhaarana, joka yhdistää eri verkot toisiinsa. Esimerkiksi lähiverkkojen kiinteät Internet-yhteydet muodostetaan reitittimen avulla. Reititin siirtää sille saapuvia datapaketteja IP-osoitteiden perusteella oikeaan kohdeosoitteeseen. Reititys tapahtuu erilaisten protokollien, tarkemmin sanottuna verkkoprotokollien, perusteella. Protokollan päätehtävänä on välittää kehyksen vastaanottajan osoite reitittimelle. Reitittimet muodostavat muistiinsa kuvan verkosta, minkä perusteella ne reitittävät liikennettä. Reititin pystyy muun muassa optimoimaan parhaan mahdollisen reitin tai määritellä varareitin, mikäli paras reitti ei toimikaan. (Paananen, J. 2005, 236.)

## 3.6 Palomuuri

Palomuuri (firewall) on lähiverkon ja Internetin välissä toimiva haittaohjelmia torjuva laite tai ohjelma. Palomuurin tehtävänä on rajoittaa ulosläh-tevää sekä sisäänpäin saapuvaa liikennettä, tutkimalla IP-pakettien osoitekenttiä ja datan sisältöä. Palomuureihin ohjelmoidaan sääntöjä, joissa sallitaan tai kielletään tiettyjen porttien, osoitteiden ja protokollien käyttö. Paketit, jotka eivät ole sallittuja palomuurin säännöissä, hylätään. Palomuurin läpi ei siis pääse liikennettä, ellei sitä ole erikseen joltakin päätelaitteelta pyydetty ja se on palomuurin sääntöjen mukaisesti sallittua. Palomuuri-

na voidaan käyttää erillistä laitetta tai tietokoneelle asennettavaa ohjelmaa. Näiden kahden yhteiskäyttö on myös hyvin suosittua, jolloin tietoturvaa saadaan lisättyä. Hämeen Monitoimitileillä on käytössä sekä fyysinen että ohjelmistopohjainen palomuuri. Fyysinen palomuuri kannattaa sijoittaa sisäverkon reunalla, jolloin mahdolliset haittaohjelmat saadaan mahdollisimman nopeasti poistettua. Palomuurien heikkouksina voidaan pitää sitä, että se suojaa vain lävitseen tulevia yhteyksiä, jolloin verkkoon tunkeutuminen on mahdollista esimerkiksi langattoman yhteyden avulla tai mikäli tunkeutuja pääsee suoraan kiinteistössä oleviin koneisiin käsiksi. (Paananen, J. 2005, 403-404.)

# 4 TOIMISTOVERKON TIETOLIIKENNE

Tietoliikenne näkyy nykypäivänä lähes jokaisen yrityksen jokapäiväisessä toiminnassa. Tietotekniikan ja -liikenteen kehittyminen on helpottanut ja nopeuttanut työntekoa huomattavasti. Nykyisin sähköpostilla pystytään hoitamaan yhteydenpitoa asiakkaisiin ja lähettämään erilaisia tiedostoja vaivattomasti. Etäyhteyksien avulla töitä pystytään tekemään joustavasti paikasta riippumatta. Digitalisoitumisen myötä maailma on käynyt pienemmäksi. Yhteydenpito, laskujen maksaminen, aikojen varaaminen ja tietojen jakaminen ovat kaikki esimerkkejä, jotka pystytään nykyisin tekemään verkon kautta. Ihmiset voivat olla jatkuvasti yhteydessä toisiinsa ja hoitamaan asioitaan, olivat he sitten missä päin maailmaa tahansa.

Tässä kappaleessa käsitellään toimistoverkon tiedonsiirtoon liittyviä yleisimpiä termejä ja protokollia. Tietoliikenteeseen kuuluu paljon erilaisia protokollia ja tekniikoita, mutta kappaleen käsitteet on rajattu olennaisimpiin Hämeen Monitoimitilien lähiverkossa liikennöiviin protokolliin ja termeihin.

## 4.1 TCP/IP

TCP/IP (Transmission Control Protocol / Internet Protocol) on usean tietoverkkoprotokollan yhdistelmä, jota käytetään erityisesti Internet-liikennöinnissä. IP-protokolla on alemman tason protokolla, joka vastaa päätelaitteiden IP-osoitteista ja datapakettien reitittämisestä verkossa. IP:n päällä voidaan käyttää myös monia muita protokollia, joista TCP-protokolla on yleisin. TCP huolehtii kahden päätelaitteen välisestä tiedonsiirtoyhteydestä, pakettien järjestämisestä sekä hävinneiden datapakettien uudelleen lähettämisestä. Vaikka TCP/IP-protokollaperheeseen kuuluu monia muitakin protokollia, suurin osa verkon liikennöinnistä tapahtuu TCP-yhteyksinä IP-protokollien päällä. Tämän vuoksi protokollaperhe tunnetaan yleisesti nimellä TCP/IP

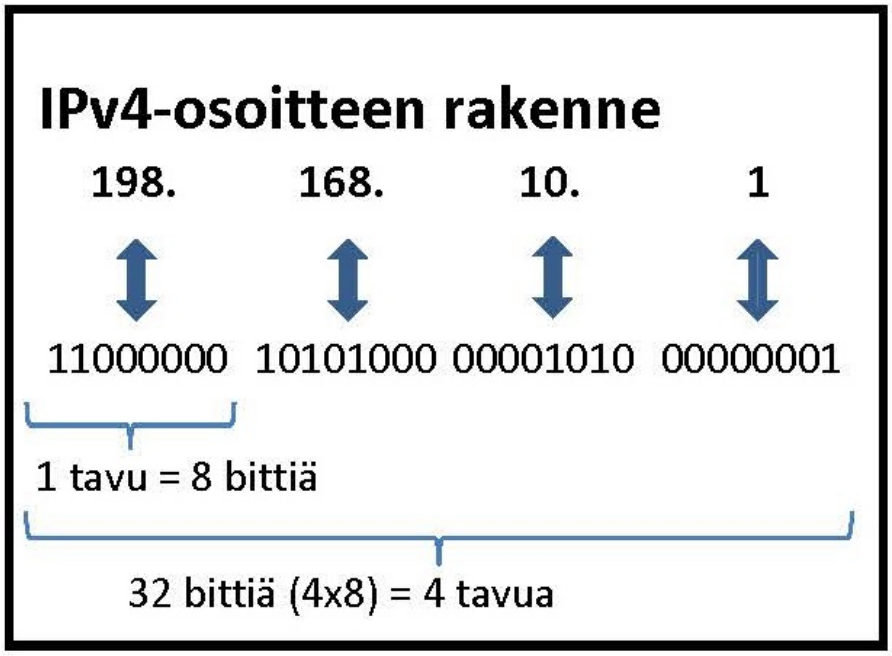
## 4.2 IP

IP (Internet Protocol) on TCP/IP-mallin Internet-kerroksen protokolla, jonka tehtävänä on huolehtia IP-tietoliikennepakettien siirtämisestä isäntäkoneelta toiselle pakettikytkentäisessä Internet-verkossa. IP ei sisällä mekanismeja, joilla tarkistettaisiin datapaketin saapuminen kohteeseen, joten paketin kulkemalla reitillä ei ole väliä. IP onkin niin sanottu yhteydetön palvelu. IP on myös koko Internetin toiminnan tärkein osa ja ainoa asia, joka yhdistää kaikkia Internetiin liitettyjä koneita. IP-paketit toimitetaan perille IP-osoitteiden perusteella. IP-osoite koostuu biteistä, jotka muodostavat numerosarjan kuten esimerkiksi: "192.168.10.1" (IPv4) tai ”2001:0db8:0000:0000:0000:0000:1420:57ab” (IPv6). WWW-osoitteiden eli verkkotunnusten muuttamisesta IP-osoitteiksi huolehtii DNS-palvelin. IP-paketit kulkevat verkon läpi kohdeosoitteeseensa ja tätä kutsutaan reitittymiseksi ja siitä huolehtivat reitittimet, jotka suorittavat reitityksen perustuen reititysprotokollien välittämään tietoihin IP-osoitteiden sijaintipai-

koista Internetissä ja lyhyimmistä reiteistä niiden välillä. (Anttila, A. 2001, 4.)

### 4.2.1 IPv4

IPv4-osoite koostuu neljästä informaatiotavusta eli 32 peräkkäisestä bitistä, joiden arvo on joko 1 tai 0. IPv4-osoitteita on siis olemassa n. 4,3 mrd kappaletta, mutta todellisuudessa kaikki osoitteet eivät ole käytettävissä, sillä IP-osoitteet on jaettu erikokoisiin luokkiin ja osa näistä on tarkoitettu yksityisiksi osoitteiksi, joilla ei liikennöidä Internetiin. IP-osoitteet kirjoitetaan yleensä pisteellisessä desimaalimuodossa, jotta ne olisivat helpompia lukea. Jokainen tavu muunnetaan siis desimaalimuotoon välille 0-255 ja nämä neljä osoitetavua erotetaan toisistaan pistein. IP-osoite voidaan jakaa kahteen osaan, joista ensimmäinen on niin sanottu verkko-osoite ja jälkimmäinen laiteosoite. Osiosta käytetään myös yleisesti nimiä verkkomaski ja aliverkko. IP-osoitteiden jakamisesta ja hallinnoimisesta Euroopassa vastaa RIPE. Kuvassa 3 on esitelty IP-osoitteen rakenne.




Kuva 3. IPv4-osoitteen rakenne

Jotta päätelaite voisi kommunikoida verkossa, tarvitsee se yksilöidyn julkisen IP-osoitteen. Mikäli jokainen verkkolaite käyttäisi omaa julkista IP-osoitetta, eivät osoitteet riittäisi kaikille. Tämän vuoksi kehitettiin NAT, jolla voidaan säästää IP-osoitteita, käyttämällä yksityisosoitteita lähiverkoissa. Osoitteiden riittämättömyyden vuoksi on kehitetty myös IPv6, jonka avulla päästään eroon muun muassa osoitteiden vajeesta. Taulukossa 4 on esitelty eri yksityisosoitealueet, joita voidaan käyttää lähiverkoissa päätelaitteiden IPv4-osoitteina. Näillä osoitteilla ei siis pysty liikennöimään Internetiin, vaan ne on muutettava julkisiksi osoitteiksi. Taulukkoon on li-

sätty myös paikallisosoitealue (localhost). Näillä osoitteilla viitataan aina tietokoneeseen itseensä.

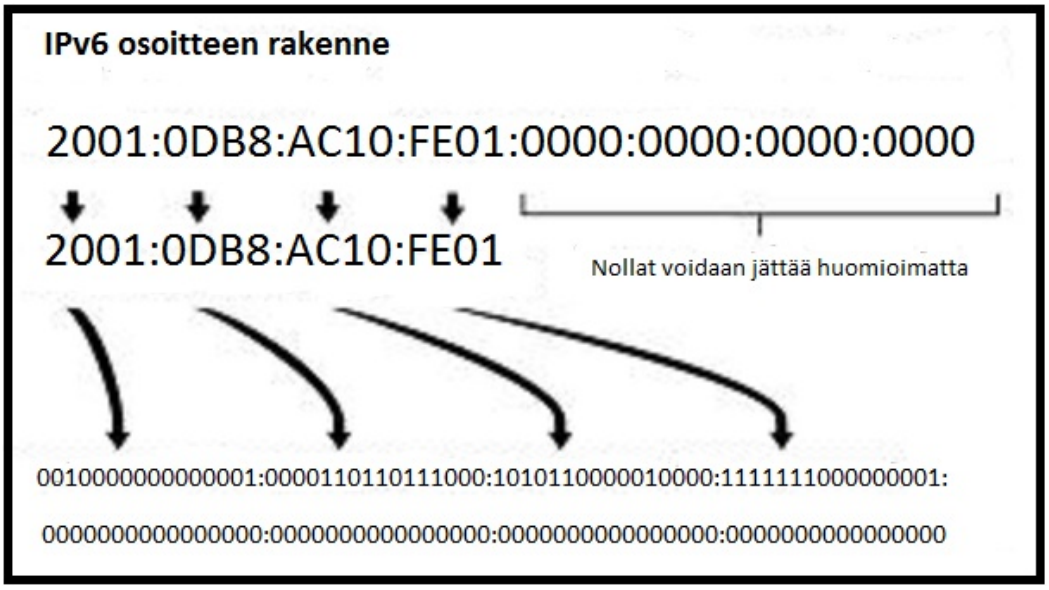
Taulukko 4. Yksityiset IPv4-osoitteet

| Verkko-osoite / verkkomaski | Osoitealue |
|---|---|
| 10.0.0.0 / 255.0.0.0 | 10.0.0.1 – 10.255.255.255 |
| 172.16.0.0 / 255.240.0.0 | 172.16.0.1 – 172.31.255.255 |
| 192.168.0.0 / 255.255.0.0 | 192.168.0.1 – 192.168.255.255 |
| 127.0.0.0 / 255.0.0.0 (localhost) | 127.0.0.1 – 127.255.255.255 |

### 4.2.2 IPv6

IPv6-protokolla on parannettu versio vanhasta IPv4-protokollasta ja se kehitetty laajentamaan nykyistä IP-osoiteavaruutta. Vanhassa IPv4-protokollassa ei ollut käytössä kuin noin 4,3 mrd osoitetta, kun taas IPv6-protokolla sisältää $2^{128}$ osoitetta, mikä on siis todella paljon enemmän kuin mitä IPv4-protokolla sisältää. Näin laaja osoiteavaruus mahdollistaa kaikille verkon päätelaitteille oman uniikin IP-osoitteen saannin. IPv6 tuo mukanaan myös monia muita ominaisuuksia, jotka omalta osaltaan helpottavat verkonhallintaa ja parantavat toimivuutta. Näistä yhtenä esimerkkinä on IPsec, joka suojaa yhteyksiä salakuunteluilta ja väärinkäytöksiltä. Internet oli alun perin tarkoitettu käytettäväksi siten, että jokaisella laitteella on oma julkinen IP-osoite. Osoitteen kuitenkin uhkasivat loppua kesken, joten kehitettiin erilaisia tekniikoita kuten NAT, joilla pystyttiin säästämään IP-osoitteita siten, että monta päätelaitetta liikennöi yhden julkisen IP-osoitteen kautta. (Anttila, A. 2001, 110-111.)

IPv6-protokollan IP-osoitteet ovat yhteensä neljä kertaa pidempiä kuin vanhemman IPv4-protokollan. Tämän vuoksi osoitteet ovat hyvin hankalia muistaa ulkoa edes desimaalimuodossa. Bittimuodossa tämä olisi lähes mahdotonta, sillä IPv6-prottokollan osoitteet koostuvat 128 bitistä. Osoitteiden muistamista varten on kehitetty useita erilaisia esitystapoja, jotta osoitteiden lukeminen ja muistaminen helpottuisi. IPv6-osoitteet kirjoitetaan kahdeksaan neljän heksatavun ryhmään, esim. 2001:410:0:1234:FB00:1400:5000:45FF. Mikäli IPv6-osoite sisältää paljon pelkkiä nollia sisältäviä tavuja, voidaan ne korvata kaksoispisteillä. Kuvassa 4 on esitelty IPv6-osoitteen rakenne.




**Kuva 4. IPv6-osoitteen rakenne**

## 4.3 TCP

TCP (Transmission Control Protocol) käyttää IP-protokollaa tarjoamaan luotettavan yhteyspalvelun kahden Internetissä olevan isäntäkoneen välille. Suurin osa Internetin tietoliikenteestä perustuu TCP-protokollaan. TCP-yhteys koostuu kolmesta vaiheesta: yhteyden luomisesta, tiedonsiirrosta ja yhteyden katkaisusta. TCP eroaa huomattavasti IP:stä, joka vain lähettää datapaketit matkaan, mutta ei varmista pääsivätkö ne perille. TCP sisältää mekanismit, joille voidaan varmistaa pakettien vastaanottamisen onnistuneen. TCP mahdollistaa myös sen, että paketit voidaan koota takaisin oikeaan järjestykseen päätelaitteella. Myös varsinaiseen dataan kohdistetut tarkistussummat muodostetaan TCP-protokollan kautta. TCP sisältää myös mekanismit, jotka säännöstelevät datavuota, jolla voidaan välttää ruuhkautumisen aiheuttamat ongelmat. TCP pyrkii hyödyntämään verkkoa mahdollisimman tehokkaasti yrittämällä luoda paketteja, jotka sisältävät mahdollisimman paljon tietoa. TCP:n päälle on rakennettu monia muitakin tärkeitä protokollia, kuten www-sivujen käyttämä HTTP (Hypertext Transfer Protocol) ja sähköpostin välitykseen käytetty SMTP (Simple Mail Transfer Protocol). (Comer, D. 2002, 209-250.)

## 4.4 DHCP

DHCP (Dynamic Host Control Protocol) on verkkoprotokolla, jonka päätehtävä on jakaa IP-osoitteita lähiverkkoon kytkeytyville laitteille. Verkon ylläpitäjä on määrittänyt tietyn IP-osoiteavaruuden reitittimen DHCP-palvelimelle, josta jokainen lähiverkkoon liittyvä laite saa käynnistyksen yhteydessä IP-osoitteen. DHCP-palvelin voi myös sijaita operaattorin verkossa. Palvelimen jakama IP-osoite on voimassa ennalta määrätyn ajan, esim. yhden vuorokauden, minkä jälkeen laite pyytää uuden osoitteen. DHCP:n käyttö yksinkertaistaa päätelaitteiden asetuksien hallintaa merkittävästi, sillä IP-osoitteita ja muita verkon käyttöön liittyviä asetuksia ei tarvitse laittaa joka koneelle manuaalisesti. DHCP-palvelin voi jakaa verkon päätelaitteille myös muitakin asetuksia, kuten nimipalvelimen IP-

osoitteen ja oletusyhdyskäytävän. Yleisesti DHCP jakaakin nämä tiedot päätelaitteille. Käytännössä DHCP-palvelin voi jakaa lähes mitä tahansa asetuksia. DHCP-palvelimelta voidaan myös rajata tietyt aliverkon osoitteet, joita ei jaeta. Tällöin näitä osoitteita voidaan käyttää tietyissä laitteissa kiinteästi. Esimerkiksi verkkotulostimille määritetään kiinteä IP-osoite. Kiinteiden IP-osoitteiden määrittäminen tietyille laitteille helpottaa verkon hallintaa. (Cisco 2003, 415-418.)

## 4.5 DNS

DNS (Domain Name System) eli nimipalvelimen tarkoituksena on suorittaa verkkotunnuksen muuttaminen numeeriseksi IP-osoitteeksi, jottei Internetiä käyttävien ihmisten tai sovellusten tarvitsisi opetella IP-osoitteita ulkoa. Nimipalvelimet ovatkin helpottaneet Internetin käyttöä merkittävästi ja niitä voidaan pitää Internetin osoitekirjoina. Internetissä kommunikoivat laitteet liikennöivät keskenään, käyttäen biteistä koostuvia IP-osoitteita, jotka ovat mallia 192.168.10.1 (IPv4). On siis helpompaa opetella muistamaan esimerkiksi osoite www.hamk.fi verrattuna palvelimen käyttämään numeeriseen IP-osoitteeseen. Nimipalvelimia käytetään myös esimerkiksi sähköpostin reitittämiseen.

## 4.6 NAT ja PAT

NAT (Network Address Translation) eli osoitteenmuunnos on Internet-tekniikka, jossa julkisesti liikennöityjä IP-osoitteita piilotetaan tai säästetään. Tekniikka kehitettiin alun perin, kun huomattiin että IPv4-osoitteet loppuvat kesken. Useimmiten osoitteenmuunnosta käytetään, kun Internet-yhteydellä ei ole kuin yksi IP-osoite, mutta useamman koneen tulisi päästä Internetiin. Kaikessa Internetiin lähetetyssä liikenteessä pitää olla julkinen, uniikki IP-osoite, jolloin tässä tapauksessa usean koneen pitää jakaa yksi osoite. Osoitteenmuunnos lisää myös lähiverkossa olevien koneiden tietoturvaa, kun yksittäinen kone ei näy lainkaan ulkomaailmaan. Ainoa asia, joka näkyy ulkomaailmaan on reititin tai palomuuri, sen mukaan kummalle laitteelle osoitteenmuunnos on suoritettu. Osoitteenmuutos tuo myös ongelmia, sillä monesti käytettäessä kaksisuuntaisia palveluja monet niistä vaikuttavat toimivan vain toiseen suuntaan, ja Internetistä takaisinpäin kulkeva liikenne jää usein tulematta perille. Tämän vuoksi NAT-laitteille voidaan määritellä avoimia yhteyksiä, jolloin laitteet pitävät niistä listaa. Yhteys poistetaan listasta, kun se suljetaan tai kun se vanhentuu. PAT (Port Address Translation) eli porttimuunnos ajaa samaa asiaa kuin NAT. Yhdellä IP-osoitteella voi olla noin 65 535 eri porttia, joiden kautta voidaan muodostaa yksittäinen yhteys, joten porttimuunnoksen avulla voidaan yhdellä yksittäisellä IP-osoitteella toteuttaa lukuisten päätelaitteiden yhteys Internetiin. (cisco.com, 2013.)

## 4.7 VPN

VPN (Virtual Private Network) eli virtuaalinen erillisverkko on tapa, jonka avulla voidaan yhdistää useampi yrityksen verkko julkisen verkon yli turvallisesti tai luoda etäyhteys yrityksen verkkoon. Yleisesti virtuaalisia

lähiverkkoja käytetään etäyhteyksien luomiseen, jolloin esim. työntekijöillä on pääsy yrityksen verkkoon myös kotiliittymän kautta. VPN-yhteyden luomiseen tarvitaan siihen sopiva laite, joka voi olla esim. reititin tai palomuuri. VPN-yhteyksien salaus voidaan toteuttaa joko fyysisellä suojauksella tai salaamalla. Salaaminen on huomattavasti yleisempi vaihtoehto, sillä se tulee huomattavasti halvemmaksi, eikä vaadi muuta kuin yhteyden julkiseen Internetiin. Salaamiseen käytetään erilaisia tunnelointiprotokollia. Yleisesti salaukseen voidaan käyttää protokollaa nimeltä IPsec. (Perlmutter, B. 2001, 10-15.)

IPsec (IP security) on suojausprotokolla, joka myös määrittää joukon eri suojausalgoritmeja sekä yleisen kehyksen. Se on joustava järjestelmä, jossa ei ole tarkkaan määritetty toimintoja ja salausalgoritmeja. Kehystä käyttäen, voivat keskenään kommunikoivat päätelaitteet valita tilanteeseen parhaiten sopivat suojausmenetelmät. IPsec soveltuu käytettäväksi verkkojen välisenä tai etäyhteyden yhteyskäytäntönä. IPsec mahdollistaa käyttäjien tunnistuksen ja suojatut palvelut IP-kerroksella ja se on yhteensopiva sekä IPv4:n, että IPv6:n kanssa. IPv6:n yleistyessä tulee IPsecin käyttökin kasvamaan. (Comer, D. 2002, 390-394.)

Etäyhteyksiä voidaan luoda myös SSL VPN-tekniikalla, joka eroaa perinteisestä VPN-yhteydestä, sillä se on toteutettu ylemmillä OSI-mallin kerroksilla 4-7 kuin esimerkiksi IPSec, jonka toiminta tapahtuu verkkokerroksella 3. IPSec pitää huolta tiedonsiirron luotettavuudesta eri salauksilla, kun SSL VPN -yhteydessä OSI-mallin kuljetuskerros 4 pitää siitä huolen. Käytännössä SSL VPN toimii siten, että asiakkaan asema ottaa yhteyden palvelimen ennalta määritettyyn porttiin ja luo SSL-tunnelin asemien välille, allokoi itselleen suljetun verkon verkko-osoitteen ja luo virtuaaliverkon näiden välille. (Cisco 2014.)

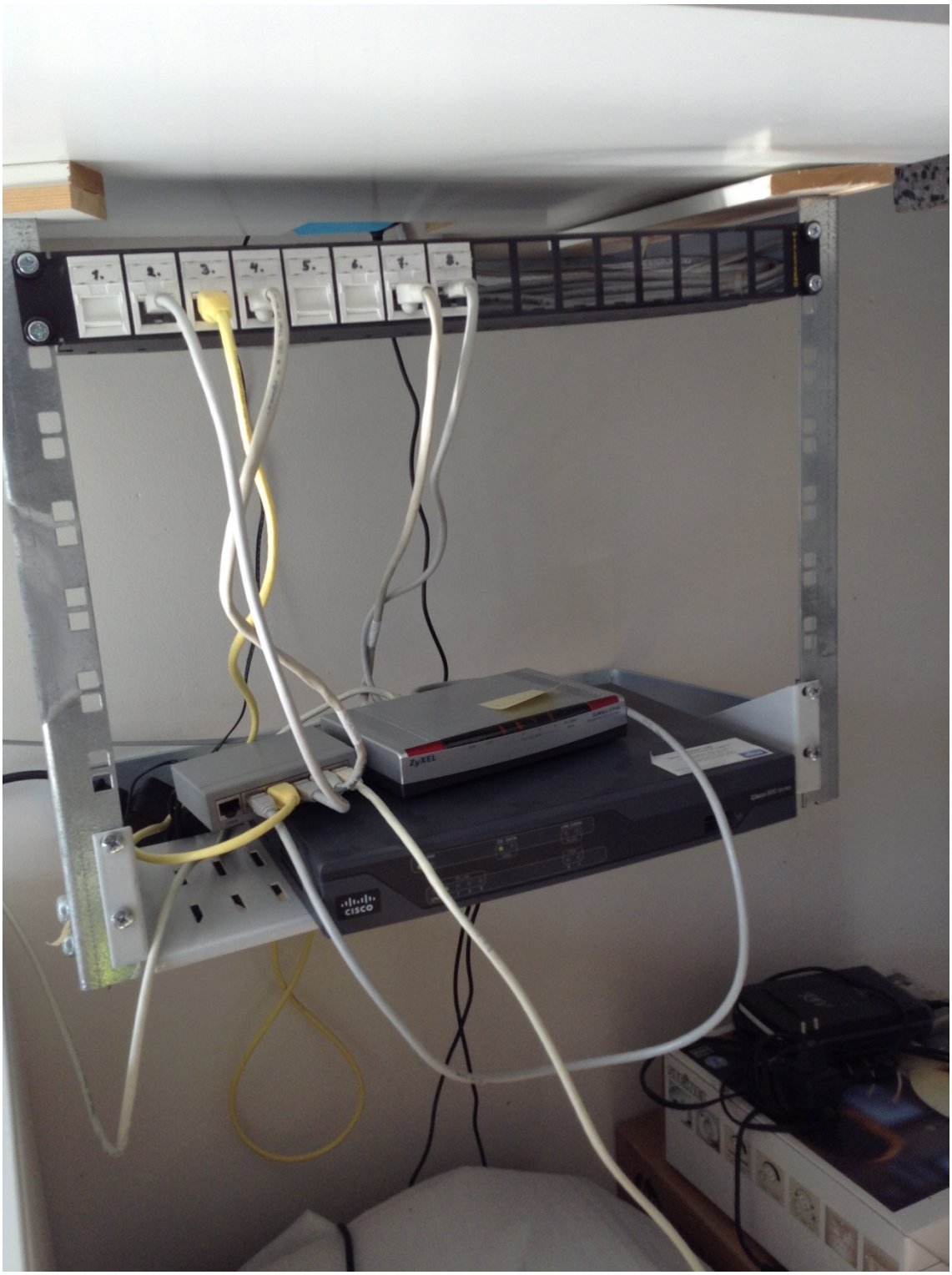
## 4.8 VLAN

VLAN (Virtual Local Area Network) on virtuaalisesti määritetty lähiverkko, jolla voidaan luoda ryhmiä, jotka voivat liikennöidä samassa fyysisessä lähiverkossa toisistaan riippumattomina ja erillisinä. Virtuaalisia lähiverkkoja käytetään yleisesti verkon segmentointiin, jolloin yrityksen eri osastot voidaan jakaa omiin lähiverkkoihinsa. Virtuaaliverkkojen avulla voidaan verkon käyttäjät jakaa pienempiin ryhmiin, jolloin myös verkon käyttöä voidaan rajoittaa käyttäjäkohtaiseksi. Tämä taas lisää osaltaan tietoturvaa, kun kaikilla käyttäjillä ei ole pääsyä kaikkiin verkon tiedostoihin ja järjestelmiin. Verkon segmentointi helpottaa myös verkon hallintaa. Jakamalla verkko virtuaalisesti voidaan myös kasvattaa tiedonsiirtokapasiteettiä ja samalla saadaan vähennettyä ylimääräistä, verkkoa kuormittavaa liikennöintiä. Eräs esimerkki virtuaalisesta lähiverkosta on yritysten, esim. ravintoloiden tarjoamat WiFi-yhteydet asiakkailleen. Tämä langaton yhteys on määritetty tietyn VLAN:n taakse, jolloin siitä ei ole pääsyä kuin ainoastaan Internetiin, mutta ei yrityksen omiin verkkoihin, jolloin yrityksen tietoturva ei vaarannu. (Jaakohuhta, H. 2005, 161.)

# 5 NYKYINEN TOIMISTOVERKKO

Hämeen Monitoimitilien toimistossa päivittäin työskentelevät työntekijät käyttävät yrityksen lähiverkkoa jatkuvasti työssään ja työnteko on lähes täysin riippuvainen verkon toimivuudesta. Verkon kaatuessa ei työnteko olisi mahdollista, sillä sähköpostin käyttö ei onnistuisi, eikä myöskään yhteydenpito asiakkaisiin onnistuisi. Myöskään kirjanpito-ohjelmien käyttö ei olisi mahdollista, sillä ne toimivat ulkoisen palvelimen kautta. Tämän vuoksi Internet-yhteyden ja lähiverkon toimintaan kannattaa panostaa, jotta pystyttäisiin välttymään mahdollisimman tehokkaasti ongelmatilanteilta, jolloin yrityksen toiminta lamautuu.

Hämeen Monitoimitilien toimistoverkko on hyvin tyypillinen Ethernet-pohjainen lähiverkko. Yrityksen kaapelointi on toteutettu suojaamattomalla kierretyllä parikaapelilla, joka rakennuksen vanhan iän vuoksi on kategoriaa Cat5e. Tämän tyypin kaapelointi on kuitenkin riittävä tämän kokoisen yrityksen tarpeisiin, sillä tiedonsiirtokapasiteetti kyseisessä kaapelissa on 1000 Mb/s. Internet-liittymä on tilattu Elisalta YritysInternet-liittymänä, jolloin Elisa hallinnoi yrityksen reititintä ja vastaa sen toiminnasta ja konfiguroinnista. YritysInternetin hyviä puolia on se, että vikatilanteissa Elisalla on vastuu ja velvollisuus korjata yhteys sopimuksessa olevan ajan sisällä. Hämeen Monitoimitileillä tämä aika on määritetty 24 tuntiin. YritysInternet on myös kätevä ratkaisu, kun yrityksen sisältä ei löydy tarvittavaa osaamista verkon hallintaan. Huonona puolena voidaan pitää sitä, että verkkoon tehtävät muutokset täytyy tilata erikseen Elisalta, sillä reitittimen konfiguraatioita ei pääse itse muokkaamaan. Internet-yhteys on ADSL-tekniikalla toteutettu ja sen maksiminopeus on 24/3 Mb/s, eli 24 Mb/s sisäänpäin tulevalle liikenteelle ja 3 Mb/s ulospäin lähtevällä liikenteelle. Reitittimenä käytetään Ciscon valmistamaa 887 VA-M reititintä. Kuvassa 5 on esitelty Hämeen Monitoimitilien kellarissa sijaitseva laitetila.




Kuva 5. Hämeen Monitoimitilien laitetila

Reitittimen rooli toimistoverkossa on erittäin olennainen, sillä sen avulla liikennöidään Internetiin. Reitittimessä suoritetaan osoitteenmuunnos, jolla yksityiset osoitteet muutetaan julkiseksi. Reititin huolehtii myös DHCP-palvelimena toimimisesta, jakamalla verkon päätelaitteille IP-osoitteet. Reititin hoitaa myös nimipalvelun tehtävän kääntämällä verkkotunnukset IP-osoitteiksi, jolloin selaimen käyttö on helpompaa, kun ei tarvitse muistaa eri sivustojen IP-osoitteita. Reitittimen päätehtävä on kuitenkin huolehtia tietoliikenteen ja datapakettien reitittämisestä verkossa.

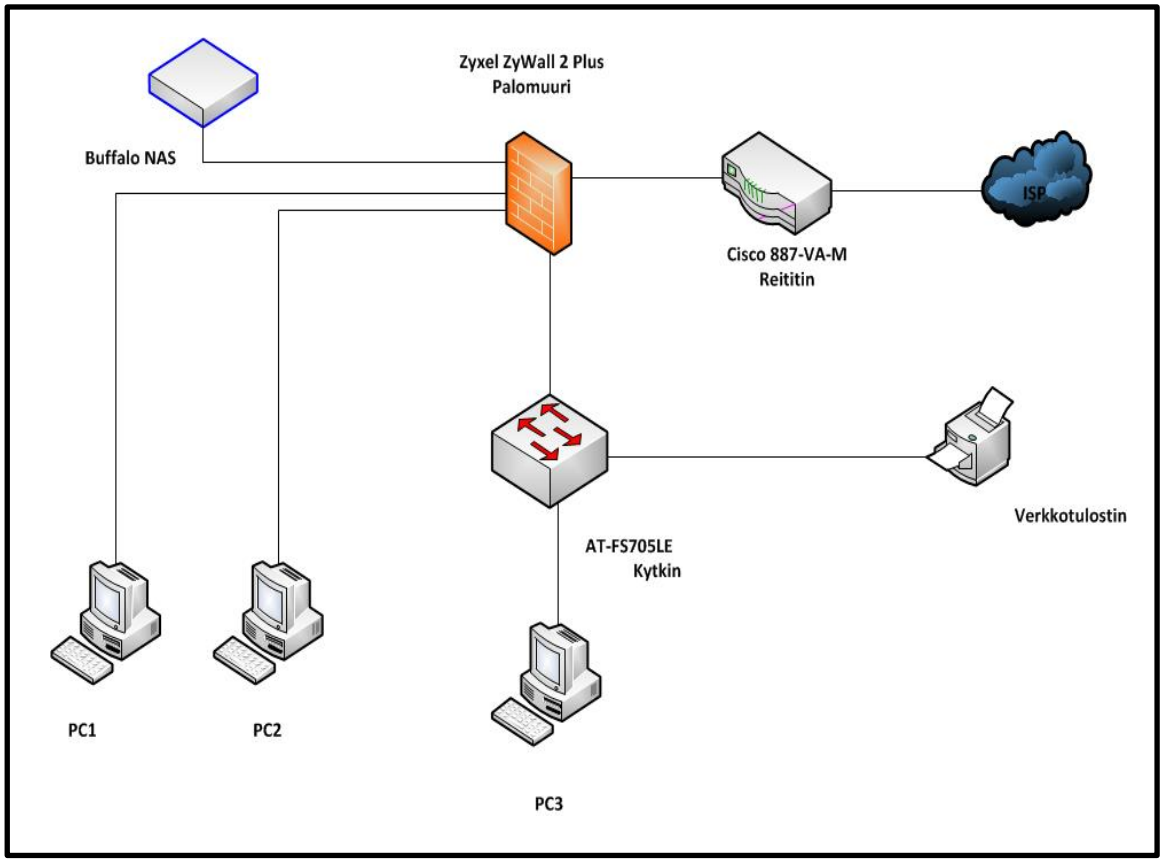
Western Systems on asentanut toimistolle Zyxelin palomuurin ja sen tehtävänä on suojata verkkoa ei-toivotuilta yhteyksiltä. Palomuuriin on määritelty asetukset, joiden mukaan vain tietyistä porteista saapuvat tai lähtevät paketit päästetään läpi. Myös vain tiettyjä protokollia käyttävät paketit päästetään kulkemaan palomuurin lävitse. Erillinen palomuuri onkin loistava tapa suojata lähiverkkoa viruksilta ja haittaohjelmilta, mutta verkon käyttäjän tulee myös olla huolellinen, jotta ei lataa verkosta haitallisia ohjelmia tai avaa epäilyttäviä linkkejä.

Hämeen Monitoimitileillä on käytössä muutamia pilvipalveluita, vaikkakin tärkeimmät tiedostot ovat säilössä ulkoisella kovalevyllä. Sähköpostin lisäksi pilvipalveluna on toteutettu kirjanpitosovellukset, jotka on ostettu palvelun tarjoajalta. Hämeen Monitoimitilien käyttämät kirjanpitosovellukset ovat Western Systemsin tarjoamia. Western Systems huolehtii myös osittain Hämeen Monitoimitilien tietokoneiden tietojärjestelmistä ja niiden ylläpidosta ja päivittämisestä. Tällä ratkaisulla on vähennetty pääoman sitomista ohjelmistoihin ja niihin liittyviin laitteistoihin. Samalla säästetään henkilöstöresursseja yrityksen kannalta tuottavampiin tehtäviin, sillä tärkeimpien ohjelmistojen ylläpidosta ja päivittämisestä ei tarvitse huolehtia itse.

Hämeen Monitoimitileillä on käytössään myös verkkotulostin, joka on yhdistetty yrityksen lähiverkkoon. Verkkotulostimen avulla tulostaminen ja asiakirjojen kopioiminen onnistuu vaivattomasti ja paperiset asiakirjat on helppo muuntaa tulostimen avulla sähköisiksi ja ne on mahdollista lähettää tulostimelta suoraan omalle pöytäkoneelle. Toimistotyössä verkkotulostin onkin hyvin olennainen osa työntekoa ja sen avulla pystytään helpottamaan monia olennaisia työtehtäviä.

## 5.1 Verkkokuva

Yrityksien lähiverkoista on hyvä laatia verkkokuva. Verkkokuvasta tulisi selvitä, miten eri verkkolaitteet kytkeytyvät toisiinsa lähiverkossa. Kunnollisen verkkokuvan laatiminen on kannattavaa, sillä se helpottaa merkittävästi vikatilojen selvittämistä ja mahdollisten ongelmien löytämistä. Etenkin isojen yrityksien lähiverkoissa, joissa verkkolaitteita on useita kymmeniä, on kunnollisen verkkokuvan laatiminen erittäin tärkeää. IT-henkilöstön vaihtuessa, pystyvät uudet työntekijät nopeasti pääsemään perille verkon kokonaiskuvasta ja toiminnasta. Verkkokuvasta olisi hyvä selvitä verkon laitteet ja niiden sijainti, sekä porttikytkennät. Kytkettyjen porttien merkitseminen on tärkeää etenkin silloin kun voidaan itse konfiguroida verkkoa. Hämeen Monitoimitilien toimistoverkon ollessa suhteellisen pieni, portit jätettiin merkitsemättä verkkokuvaan. Käytetyt portit ja kytkennät on kuitenkin kirjattu erilliseen liitteeseen 1. Hämeen Monitoimitilien verkkokuva ennen muutoksia on esitelty kuvassa 7.




Kuva 6. Hämeen Monitoimitilien verkkokuva

# 6 TULEVAISUUDEN LÄHIVERKOT

Tulevaisuuden ennustaminen on vaikeaa, mutta erityisen haastavaa ja vaikeata se on todella nopeasti muuttuvalla ja kehittyvällä tietoliikennetekniikka-alalla. Katsottaessa tietotekniikan historiaan, huomataan että kehitys on ollut nopeaa viime vuosikymmeninä ja tulee mitä todennäköisimmin jatkumaan samankaltaisena. Tiedonsiirtokapasiteetti on moninkertaistunut ja verkon päätelaitteiden määrä jatkaa kasvamistaan. Internetin käytöstä on tullut osa ihmisten arkea ja tänä päivänä internetyhteys onkin lähes välttämätön. Yritysten tiedostot ja palvelut ovat siirtyneet verkkoon ja ne ovat käytettävissä lähes missä tahansa ja milloin vain. Tässä vain muutamia esimerkkejä. Internet tulee siis leviämään kaikkialle ja kaikille. Ihmisten elämä tulee olemaan jatkuvasti yhä enemmän tietotekniikan varassa ja ihmisillä tulee olemaan yhä useammin yhteys Internetiin, mitä erilaisimmissa paikoissa. Nykyisin langattomia lähiverkkoja on rakennettu jo esimerkiksi juniin ja kauppakeskuksiin, ja tulevaisuudessa langattomat verkot tulevat laajenemaan entisestään.

Tulevaisuuden Internetissä henkilökohtainen informaatio on aina ja kaikkialla saatavilla ja Internet kuuluu osana jokapäiväiseen ympäristöömme. Internetin arkkitehtuuri tulee myös olemaan erilainen ja uudistunut ja siitä on tullut käyttäjäkohtaisempi, perustuen käyttäjäkohtaisiin tietoihin. Internetin avulla voidaan hallinnoida lähes kaikkea, mutta tämä vaatii saumattomuutta järjestelmien välillä ja täysin uudenlaisia verkkoinfrastuktuureja. Langattomien tiedonvälitysjärjestelmien tiedonsiirtokapasiteetin on oltava huomattavasti nykyistä suurempia, jotta jatkuvasti kasvavan tietomäärän käsittely onnistuisi sujuvasti. Uudenlainen Internet mahdollistaisi lukemattomia määriä erilaisia uusia palveluita ja arkea helpottavia toimintoja. Internetin kehityksen myötä on mahdollista, että esimerkiksi tablettilaitteet hakevat eri verkkosivustoilta käyttäjää kiinnostavat artikkelit valmiiksi avausnäytölle. Kahvinkeitin voidaan ohjelmoida keittämään sopiva määrä kahvia oikeaan aikaan, perustuen talossa olevien henkilöiden määrään ja heidän sähköisiin kalenterimerkintöihinsä. Autolla ajaessa, auto muistuttaisi postitoimiston kohdalla noutamattomasta paketista ja kertoisi parhaan reitin perustuen tieverkoston ruuhkatilanteisiin. Työpaikalla ovet avautuisivat taskussa olevan tunnistimen avulla automaattisesti ja tietokone ilmoittaa, kun tapaamiseen saapuva henkilö saapuu rakennukseen. Yksinkertaisesti sanottuna kaikki tapahtuu verkossa ja kaikki ovat verkossa, ihmiset ja esineet. Erilaisten esineiden liittämistä Internetiin kutsutaankin termillä Internet of things, ja tämä tulee varmasti yleistymään lähitulevaisuudessa. Tulevaisuudessa verkon käyttö tulee olemaan paljon laajempaa ja monipuolisempaa ja rajoja tälle kehitykselle on vaikea keksiä. (Teknologiateollisuus 2010.)

Vaikka tulevaisuuden Internet ja lähiverkot saattavatkin olla osana lähes kaikkea ja kaikkia, ei näin suuri mullistus kuitenkaan tule tapahtumaan muutaman vuoden sisällä, sillä tämänhetkinen verkkoinfrastuktuuri ei sitä täysin mahdollista ja monien jo olemassa olevien tekniikoiden käyttö on varsin kallista. Kehitystä on vielä tapahduttava, mutta mikäli tietotekniikan kehitys jatkuu samanlaisena kuin aiempina vuosikymmeniä, niin Internetin ja lähiverkkojen mahdollisuudet ovat suuret. Seuraavissa luvuissa

pyritään käsittelemään tämän hetken ja lähitulevaisuuden kehitystä tietoliikenteen saralla, lähtökohtana Hämeen Monitoimitilien lähiverkko. Tämän hetken kolme suurinta lähiverkon kehitykseen vaikuttavaa tekijää ovat tiedonsiirtokapasiteetin kasvu, verkon varmatoimisuus ja langattomuus. Lisäksi IPv6:n jatkuvasti laajeneva käyttö ja sen mahdollistamat uudet ominaisuudet ovat hyvinkin ajankohtainen aihe. Toinen yksittäinen muuttuja, jota Hämeen Monitoimitilienkin käyttöön voisi kuvitella, on pilvipalvelu, jolla voidaan varmistaa yritysten tiedostojen säilyvyys ja käyttö paikasta riippumatta.

## 6.1 Tiedonsiirtokapasiteetti

Tiedonsiirtokapasiteetti on kymmenkertaistunut useita kertoja viimeisten vuosikymmenien aikana. Ethernetin ensimmäinen versio, joka kehitettiin 1972, ja jota kutsuttiin ALOHAnetiksi, käytti siirtonopeutena 2,94 Mb/s. 1980-luvulla verkon nopeus oli jo yli kolminkertaistunut, ja tänä päivänä käytetään jo kymmenien gigabittien nopeuksia. Mikäli kehitys jatkuu samanlaisena, tulee tiedonsiirtonopeus kasvamaan jatkossakin. Tosin tiedonsiirtomedioiden fyysiset ominaisuudet saattavat toimia rajoittavana tekijänä nopeuden kasvamisen suhteen, mutta myös eri tiedonsiirtomedioiden kehitys on jatkuvaa. Tiedonsiirtokapasiteetin kasvu onkin hyvin todennäköisesti isossa roolissa tulevaisuuden lähiverkoissa ja kapasiteetin kasvu tulee olemaan tärkeää, jotta uudenlaisia sovelluksia voidaan ottaa käyttöön.

Tulevaisuudessa tarve langattomille päätelaitteille tulee kasvamaan, etenkin sellaisten joiden tiedonsiirtokapasiteetti on moninkertainen verrattuna nykypäivän tarpeisiin. Yksi ratkaisu tiedonsiirtonopeuden kasvattamiseen on käyttää niin sanottua moniantennitekniikkaa, jossa tiedonsiirto toteutetaan useiden toisistaan riippumattomien antennien välityksellä. Langattomat päätelaitteet tukevat tälläkin hetkellä eri standardeja, mutta tulevaisuuden langattomissa päätelaitteissa tuetaan useampia eri standardeja suurelle määrälle eri radiorajapintoja, kuten eritaajuuksilla toimiville matkapuhelinjärjestelmille ja langattomille lähiverkoille. Laitteiden tulisi kuitenkin olla mahdollisimman pieniä ja ylimääräistä tilaa ei ole. Tämän vuoksi ei ole järkevää käyttää erikseen jokaiselle standardille omaa antennia. Yksi järkevistä ratkaisuista on käyttää laajakaistaisia antenneja, joilla voidaan tukea mahdollisimman monia langattomia tiedonsiirtostandardeja ja samalla päätelaitteen koko ei kasva liian suureksi. Langattomien päätelaitteiden asentaminen on helpottunut PoE (Power over Ethernet) tekniikan myötä. Tällä tekniikalla voidaan syöttää virtaa päätelaitteeseen kierretyllä parikaapelilla Ethernet-portin kautta, jolloin päätelaitteen ei tarvitse sijaita pistorasian lähellä. (Sonkki, M. 2013.)

Tällä hetkellä elämme maailmassa, jossa tiedonsiirtokapasiteetti on melko rajattua, mutta infrastuktuurikehitystä tulisikin miettiä silmällä pitäen mahdollisuutta korkeampaan tiedonsiirtokapasiteettiin, sillä tulevaisuudessa lähiverkkojen käytön rajoitukset eri sovelluksissa ja käyttötarkoituksissa tulevat vähenemään tai jopa poistumaan. Tiedonsiirtokapasiteetin kasvun jatkuessa samalla vauhdilla kuin tähänkin asti, on vaikea kuvitella mitä kaikkea lähiverkkojen avulla voidaan tehdä. Verkossa toimivien sovel-

lusten ja toimintatapojen määrää tulee joka tapauksessa kasvamaan tiedonsiirtokapasiteetin kasvaessa.

## 6.2 Verkon varmatoimisuus ja laatu

Tärkeitä palveluita siirretään verkkoon Internetin ja lähiverkkojen kasvaessa. Samalla kasvaa tarve palveluiden varmatoimisuudelle ja laadulle. Esimerkiksi tilanteessa, jossa tietyn rakennuksen toiminnot, kuten ovien avautumien, sähköt, ilmastointi, ovat verkon varassa, täytyy verkon olla varmatoiminen ja laadukas, sillä varaa katkoksiin ei ole. Tämän vuoksi tietoverkkojärjestelmiin rakennetaan erilaisia varmistuksia ja varajärjestelmiä, jotta tietojen säilyminen ja palveluiden toimiminen olisi varmaa. Tavoitteena on, että esimerkiksi konesalien palvelimia voidaan vaihtaa ilman käyttökatkoksia, sillä muut palvelimet korvaavat automaattisesti vioittuneen palvelimen. Tällöin verkko säilyy viasta huolimatta toimintakuntoisena ja vikasietoisuus on korkea. Konesaleista tehdään myös kriisisietoisia, ja ne pyritään sijoittamaan turvallisiin ympäristöihin, joissa on riittävästi energiaa ja jäähdytystä tarjolla, sekä useita varmoja tiedonsiirtoreittejä verkkoon. Tästä esimerkkinä on Googlen palvelinkeskus Haminassa.

Lähiverkoissa tiedon eheys ja yhteyksien toimintavarmuus voidaan varmistaa varmentamalla yhteydet ja klusteroimalla kriittisimmät verkkolaitteet, kuten palomuurit. Klusteroinnilla tarkoitetaan periaatteessa laitteen kahdentamista, jolloin päälaitteen vioittuessa tiedonsiirto tapahtuu automaattisesti varalaitteen kautta. Lähiverkkoihin rakennetaan myös varayhteyksiä verkon toiminnan parantamiseksi. Kuvassa 1 esitellyssä yleiskaapeloinnin rakennekuvassakin on kuvattu varayhteydet eri jakamoiden välille, jolloin yhden linjan vioittuminen ei kaada koko verkon toimintaa.

## 6.3 Langattomuus

Langattomuus on tähän mennessä mahdollistanut monenlaisten laitteiden liittämisen verkkoon ja niiden käytön mobiilisti. Langattomuus mahdollistaakin tulevaisuudessa ns. jokapaikan tietotekniikan (engl. Ubiquitous computing), mikä tarkoittaa huomaamattomasti toimivaa ja ympäristöönsä sulautuvaa kaikkialla olevaa tietotekniikkaa, jolla taas viitataan myös Internet of things käsitteeseen, eli erilaisten laitteiden liittäminen Internetiin. Jokapaikan tietotekniikka ei häiritse käyttäjää, eikä keskeytä muuta toimintaa. Se toimii ihmisten ja yritysten arkitoimissa kaikkialla ja koko ajan. Kodin ja toimiston esineet ja koneet viestivät langattomasti keskenään ja pystyvät muokkaamaan toimintaansa myös itsenäisesti. Ubiquitous computing voidaan myös suomentaa termillä läsnä-äly. (Eduskunta 2008.)

Langattomuus mahdollistaa uusia tekniikoita ja sovellutuksia ja näiden kasvu on viime vuosina ollut suurta ja tulee myös jatkumaan samankaltaisena. Langattomien laitteiden käyttö on jo nyt osa ihmisten arkea, mutta se tulee olemaan yhä isompi osa ihmisten arkea, verkkoon liitettävien laitteiden määrän kasvaessa ja sovellutuksien kehittyessä. Langattomuus kasvaa lähiverkoissa, mutta myös matkapuhelinverkoissa, joissa 4G-yhteyksien yleistyminen ja älypuhelimien kehittyminen ovat isossa nosteessa.

Langattomuus ei kuitenkaan välttämättä leviä aivan kaikkialle, sillä ihmisten yksityisyys saattaa olla vaarassa. Esimerkiksi Suomessa on suunniteltu autojen satelliittiseurantaa, jonka mukaan voitaisiin toteuttaa verotusta, mutta mahdollisuus liikkua vapaasti ilman seurantaa on oikeus, josta moni ei ole valmis luopumaan autoverouudistuksen yhteydessä tai missään muussakaan yhteydessä. Myöskin RFID-sirut (Radio Frequency IDentification), jotka ovat etätunnistukseen tarkoitettuja pieniä laitteita, saattavat kohdata vastarintaa tietyillä markkinoilla. Siruja on jo suunniteltu asennettavaksi esimerkiksi älyvaatteisiin, jotka voisivat toimia esimerkiksi välittämällä tietoa omistajan mieltymyksistä hänen astuessaan myymälään. RFID-siruja käytetään jo tälläkin hetkellä moniin eri tarkoituksiin, mutta ihmisten yksityisyydensuojan ja tarve yksityisyydelle, voivat estää sirujen yleistymistä eri esineisiin.

## 6.4 IPv6 hyödyt lähiverkoissa

IPv6 tulee olemaan ehdottomasti yksi isoimmista muutoksista ja uutuuksista tietotekniikan lähitulevaisuudessa. IPv6:n käyttöönotto tulee myös olemaan jossakin vaiheessa lähes pakollista, sillä verkkolaitteiden määrä kasvaa jatkuvasti, mikä taas aiheuttaa IPv4-osoitteiden loppumisen. Suurin tekijä verkkolaitteiden kasvuun on se, että yhä useampia ja erilaisempia laitteita liitetään Internetiin. Suomessakin useimmat verkko-operaattorit ovat jo varanneet oman IPv6-lohkonsa, josta osoitteita jaetaan. IPv6-osoitteiden tilaaminen yrityksille onnistuu jo ainakin TeliaSoneralta. Toistaiseksi IPv6:n käyttöönotto yrityksissä on vielä vähäistä, mutta IPv6:n yleisyys tulee kasvamaan rajusti lähivuosien aikana. IPv6:n käyttöä on toistaiseksi vältelty, sillä osoitteenmuunnoksella on IP-osoitteet saatu riittämään. IPv6 ei myöskään tällä hetkellä ole tuettu aivan kaikissa käyttöjärjestelmissä, verkkolaitteissa ja ohjelmistoissa, mutta alan merkittävimmät valmistajat kuten Cisco, IBM, Microsoft ja Nokia ovat ilmaisseet tukensa protokollalle ja kehittävät jatkuvasti yhteensopivuutta uusiin ja vanhoihin laitteisiin. Vaikkei IPv6-protokollaa käyttäviä palveluita tai verkkoja vielä laajamittaisesti ole otettukaan käyttöön, tulee niiden käyttöönotto väistämättä vastaan lähivuosina. IPv6:sta välttämättömän tekee osoitteiden loppuminen kesken, mutta se tuo mukanaan myös muita uudistuksia.

IPv6 yksinkertaistaa lähiverkkojen rakennetta ja reititystä merkittävästi. Reititystaulut pienenevät ja reititys muuttuvat tehokkaammaksi ja hierarkiseksi. IPv6 sallii lähiverkon eri osien muutoksen yhdeksi verkoksi, jota mainostetaan Internetiin päin. IPv6-kehystä on myös muutettu siten, että pakettien käsittely on tehokkaampaa ja nopeampaa. IPv6 ei sisällä IP-kerroksen tarkistussummaa, joten sen laskemiseen ei kulu aikaa jokaisella reitin varrella olevalla laitteella. Nopeampi pakettien käsittely tulee tarpeelliseksi yhä kasvavissa langattomissa lähiverkkototeutuksissa. IPv6 parantaa myös päätelaitteiden liikkuvuutta langattomissa verkoissa. Esimerkiksi hyvin toteutetussa IPv6-ratkaisussa päätelaitteen liikkuessa toisesta langattomasta verkosta toiseen tai siirtyessä 3G-yhteyteen, eivät verkon kautta toimivat sovellukset huomaa tätä laisinkaan. IPv6 tukee myös suoratoistoa eli streamausta paremmin kuin IPv4, joka mahdollistaa datan lähettämisen ja samaan aikaan katsomisen reaaliaikaisesti verkon yli. Paket-

teja voidaan lähettää useisiin kohteisiin samanaikaisesti, verkkokaistaa säästäen. IPv6-otsikko sisältää kentän, jolla päätelaite tunnistaa pakettien kuuluvan samaan lähetysvirtaan, jolloin pakettien käsittely nopeutuu. (ipv6.willab.fi, 2008.)

IPv6 sisältää myös verkkoasetusten automaattisen konfiguroinnin, jolloin päätelaite etsii automaattisesti yhteyden Internetiin reitittimen kautta. Päätelaite myös muodostaa oman IPv6-osoitteensa automaattisesti, mutta nimipalvelu on konfiguroitava erikseen. Myös verkko-operaattorin vaihtuessa voidaan osoite vaihtaa lennosta vanhojen tippuessa pois ja uusien tullessa tilalle automaattisesti. Osoitteenmuunnoksen jäädessä historiaan, ja jokaisen verkon laitteen saadessa oman yksilöllisen IPv6-osoitteen, muuttuu verkko yksinkertaisemmaksi. Yksilölliset IPv6-osoitteet mahdollistavat suorien päästä päähän yhteyksien luomisen helposti, mikä avaa mahdollisuuden uusien sovelluksien käytölle. Suorat päätelaitteiden väliset yhteydet parantavat myös nykyisten palvelujen, kuten VoIP:n ( Voice over Internet Protocol) käyttöä. (Desmeules, R. 2007.)

IPsecia (IP Security) käytetään suojaamaan salaamatonta liikennöintiä julkisen verkon ylitse yhdistämään esimerkiksi kahta eri toimipaikkaa. Tällöin liikenne salataan, tunneloidaan ja sille lasketaan tarkistussumma, jonka avulla tiedon koskemattomuus voidaan tarkistaa. IPsec-tuki on osa IPv6 toteutusta, minkä avulla sovellukset voivat salata liikenteen neuvottelemalla salauksen päästä päähän. IPsecin avulla voidaan siis luoda helposti ja turvallisesti VPN-yhteyksiä, mutta sitä voidaan käyttää myös mm. langattomien WLAN-verkkojen suojaukseen. (Dunmore, M. 2005.)

## 6.5 Pilvipalvelut

Pilvipalvelulla tarkoitetaan jossakin päin Internetiä sijaitsevaa palvelua, joka on useimmiten ulkoistettu palvelu ulkomailla. Pilvipalveluita ovat muun muassa sähköposti, tallennustila, sekä pilvessä sijaitsevat erilaiset sovellukset. Pilvipalveluita on saatavilla sekä julkisina, että yksityisinä palveluina. Tavallisen kuluttajan on mahdollista käyttää pilvipalvelimella olevia toimisto-ohjelmia esimerkiksi nettiselaimella ja yleisin pilvipalvelu on sähköposti. Myös Facebookia voidaan pitää eräänlaisena pilvipalveluna, sillä sinne on mahdollista tallentaa esimerkiksi kuvia, jotka ovat saatavilla missä vain. Tällä hetkellä on meneillään pilvipalveluiden arkipäiväistyminen. Moni yritys harkitsee tai on jo siirtynyt käyttämään pilvipalveluita, vaikka se on vieläkin kohtuullisen uusi asia yrityksille. Yrityksien kannalta epäilyttävää voi olla se, että heidän tietonsa ulkoistetaan ulkomaille johonkin pilveen. Riskinä voidaan myös pitää tietojen mahdollista väärinkäyttöä tai tietovuotoa palveluntarjoajan verkossa. Pilvipalvelut ovat kehittyneet hitaasti, mutta kehitys on nopeutunut lähivuosina huimaa vauhtia. Yhä useampi yritys siirtyy käyttämään pilvipalveluita niiden kilpailukykyisen hinnoittelun ansiosta ja koska niitä ovat helppo ylläpitää, sillä päivitys ja ylläpito tapahtuvat palveluntarjoajan puolesta. Suosittuja arkikäytössä olevia pilvipalveluita ovat esimerkiksi tallennustilaa tarjoavat mm. Dropbox, Google Drive ja Microsoft Skydrive. Google ja Microsoft ylläpitävät myös pilvessä käytettäviä toimisto-ohjelmia. (Salo 2010, 3.)

# 7 KEHITYSIDEAT

Hämeen Monitoimitilien verkkoon olisi mahdollista tehdä paljonkin muutoksia, mutta kaikkien muutoksien tuoma hyöty ei välttämättä kattaisi muutoksen aiheuttamia kuluja. Esimerkiksi IPv6:n käyttöönottoa ei ole vielä toistaiseksi suunniteltu, koska sillä saavutettavat hyödyt olisivat melko pienet kyseiselle yritykselle. IPv6:n käyttöönotto tosin saattaa tulla kyseeseen sen käytön yleistyessä. Tiedonsiirtokapasiteetti todettiin myös riittäväksi, joten toimintaa päätettiin jatkaa nykyisellä liittymällä. Tässä luvussa on esitelty Hämeen Monitoimitilien lähiverkkoon tehtävät muutokset.

## 7.1 WLAN-verkon hankinta

Hämeen Monitoimitileille päätettiin hankkia langaton verkko toimistolle. Työkoneiksi on hankittu pöytäkoneiden lisäksi yksi kannettava tietokone, jolla verkkoon voidaan liittyä langattomastikin. Lisäksi langatonta verkkoa tarvitaan mobiililaitteiden, kuten älypuhelimien Internet-yhteyksien luomiseen. Langaton Internet-yhteys annetaan käyttöön myös toimistolla päivittäin käyville asiakkaille, jotta heillä on mahdollisuus käyttää Internetiä tarvittaessa. Asiakkaille tarjottava Internet-yhteys rajoitettiin kuitenkin erilliseen virtuaaliseen lähiverkkoon, josta ei ole pääsyä yrityksen tiedostoihin. Täten tietoturva ei vaarannu, vaikka asiakkaat pääsevätkin yrityksen verkon kautta Internetiin. Langattoman verkon käyttöönotto toteutettiin yhdessä Elisan kanssa.

Langaton tukiasema asennettiin toimistotilaan. Toimitilan pienestä koosta johtuen, ei tukiaseman paikkaa tarvinnut suunnitella, sillä kuuluvuus kattaa koko tilan. Tukiasemaan määritettiin tarvittavat asetukset ja salasanat, sekä luotiin kaksi erillistä langatonta verkkoa. Reitittimeen tilattiin Elisalta konfigurointimuutos, jossa langattoman verkon virtuaaliverkot eriteltiin siten, että vierailijaverkosta on pääsy ainoastaan Internetiin.

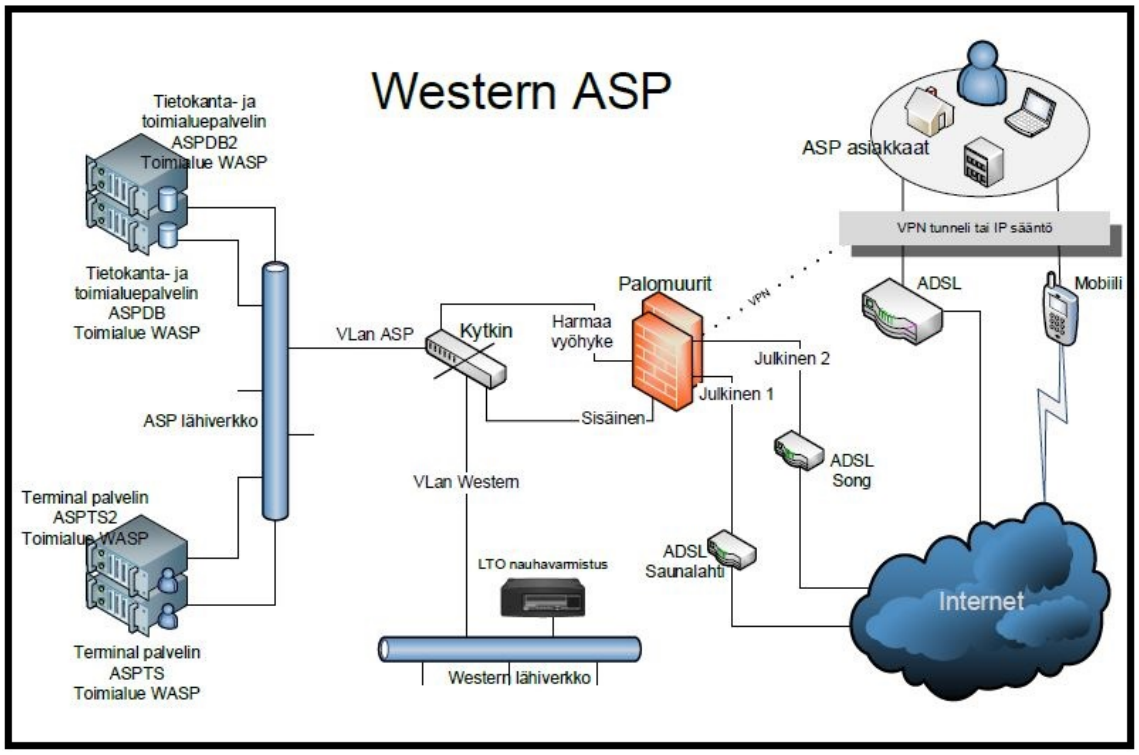
## 7.2 Tietoturva

Yrityksen tietoturvan todettiin olevan kunnossa ja palomuurin säännöstöt todettiin toimiviksi. Työkoneiden virustorjunta kuitenkin tarkistettiin ja päivitettiin ajan tasalle, jotta tietoturva olisi taattua. Langattoman lähiverkon tietoturvallisuus on taattu vahvalla salasanalla ja erottelemalla asiakkaille tarjottu verkko erilliseen virtuaaliseen lähiverkkoon, josta ei ole pääsyä yrityksen tiedostoihin.

## 7.3 Etäyhteydet

Hämeen Monitoimitileille päätettiin luoda etäyhteys Western Systemsin palveluihin yrityksen omistajan kotikoneelle. Etäyhteyteen käytettiin Microsoftin RDP-yhteyttä (Remote Desktop Control), jonka avulla päästään käsiksi virtuaaliseen työpöytään, jossa voidaan käyttää kirjanpito-ohjelmistoja. Salattu yhteys Hämeen Monitoimitilien tietokoneen ja Westernin järjestelmän välille luodaan Watchguardin SSL VPN – sovelluksel-

la, joka asennettiin käyttäjän tietokoneelle. Etäyhteys luotiin yhteistyössä Western Systemsin kanssa. Yhteys luodaan asiakkaan verkosta Internetin kautta Westernin palomuuriin. Yhteys luodaan VPN-tunnelin avulla, jolloin yhteys pysyy salattuna. Kuvassa 8 on esitelty Western Systemsin verkkokuva, josta selviää etäyhteyden toiminta.



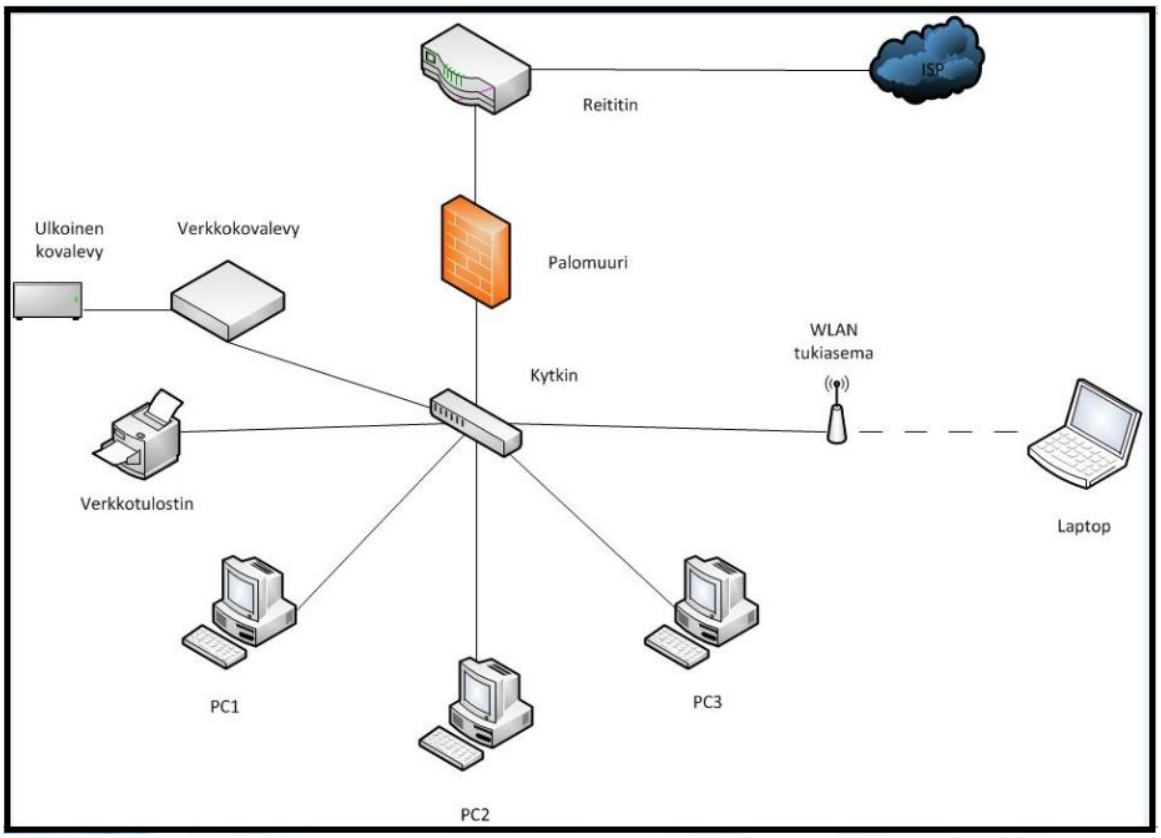

Kuva 7. Etäyhteys Western Systemsin järjestelmiin

## 7.4 Kovalevyn varmentaminen

Buffalon verkkokiintolevyyn liitettiin USB-portin kautta ulkoinen kiintolevy. Ulkoiselle kiintolevylle on Buffalon NAS-aseman hallintaohjelmiston avulla määritetty kerran viikossa tehtäväksi varmuuskopio verkkokiintolevyllä sijaitsevista varmuuskopioiduista tiedostoista. Mikäli Buffalon verkkokiintolevy sattuisi menemään rikki, tällöin tiedostot ovat tallessa ja turvassa myös ulkoisella kiintolevyllä.

## 7.5 Uusi verkkokuva

Toimistolle päätettiin myös hankkia lähitulevaisuudessa uusi kytkin, jonka myötä verkon rakennetta saadaan yksinkertaistettua. Kaikkien tehtyjen ja tulevien muutoksien jälkeen Hämeen Monitoimitilien uusi verkkokuva tulee olemaan kuvan 9 mukainen.




**Kuva 8. Hämeen Monitoimitilien uusi verkkokuva**

# 8 TULOKSET JA YHTEENVETO

## 8.1 Tulokset

Tässä opinnäytetyössä tutkittiin Hämeen Monitoimitilien lähiverkkoa ja sen rakennetta. Tavoitteena oli saada selkeä kuva lähiverkon toiminnasta ja toteuttaa ja suunnitella muutoksia, joilla lähiverkkoa ja sen toimintaa voitaisiin parantaa. Lähiverkon toiminta todettiin toimivaksi ja Elisan ja Western Systemsin hallinnoimien ominaisuuksien olevan kunnossa. Muutamia parannuksia ja muutoksia kuitenkin onnistuttiin toteuttamaan, osa yhteistyössä yrityksen lähiverkosta vastaavien yrityksien kanssa. Yritykseltä oli esitetty toiveita langattomasta lähiverkosta ja mahdollisuudesta työskennellä myös kotoa käsin. Nämä toiveet saatiinkin toteutettua onnistuneesti, joten tämän puolesta työ oli onnistunut. Lisäksi verkkokovalevy varmennettiin rikkoutumisen varalta ja toimistoverkon ohjelmistoja päivitettiin.

Opinnäytetyössä tutkittiin myös lähiverkkojen kehitystä lähitulevaisuudessa. Lähitulevaisuuden kolmeksi tärkeimmäksi kehityssuunnaksi todettiin tiedonsiirtokapasiteetin kasvu, langattomuus ja verkon toimintavarmuus ja laatu. Myös IPv6:n jatkuvasti lisääntyvä käyttöönotto ja sen tuomia hyötyjä pohdittiin lähiverkkojen kehityksen kannalta. Vaikka tulevaisuutta onkin äärimmäisen vaikea ennustaa, onnistuttiin työssä esittämään lähiverkkojen todennäköisiä kehityssuuntia ja trendejä, perustuen luotettaviin lähteisiin.

## 8.2 Yhteenveto

Työ oli erittäin opettavainen ja tietoisuus lähiverkoista ja niiden toiminnasta syveni huomattavasti, verrattuna opintojen aikana saatuun koulutukseen. Sain paljon uutta ja arvokasta tietoa lähiverkoista, Ethernetistä, IP/TCP-protokollista ja etenkin IPv6 toiminnasta ja ominaisuuksista. Tulevaisuuden lähiverkkojen tutkiminen avasi silmät uusille mahdollisuuksille ja sovellutuksille, jotka voivat olla mahdollisia toteuttaa langattomasti lähiverkoissa. Tämän aiheen tutkiminen olikin erittäin mielenkiintoista ja antoisaa, ja uskon, että tässä työssä saatu tietämys tulee olemaan hyödyksi myös jatkossa. Opin myös paljon asioita, joita voin käyttää hyväksi nykyisessä työssäni.

Aluksi työn rajauksessa oli ongelmia, mutta onneksi löytyi sopivan kokoinen yritys, jolle sain tehdä tämän opinnäytetyön. Myös yhteistyö Hämeen Monitoimitilien lähiverkkoa ylläpitävien yrityksien kanssa oli joustavaa ja saumatonta, tosin Elisa ei sallinut pääsyä reitittimen konfigurointitietoihin, mutta työn tekeminen onneksi onnistui tästä huolimatta. Haluaisinkin kiittää kaikkia tässä työssä mukana olleita ja etenkin Hämeen Monitoimitilien henkilökuntaa, joka päästi minut tutkimaan laitetilaansa ja muita päätelaitteita lukuisat kerrat.

# LÄHTEET

Anttila, A. 2001. TCP/IP tekniikka. 2.korjattu painos. Helsinki: WS Bookwell

Cisco Networking Academy Program 2003. CCNA1 and 2 Companion Guide. USA: Cisco Press

Comer, D. 2002. TCP/IP Jyväskylä: Gummerus Kirjapaino Oy

Desmeules, R. 2007. Cisco Self-Study: Implementing IPv6 Networks (IPv6). 3. painos. Yhdysvallat: Cisco Press.

Dunmore, M. 2005. 6net: An IPv6 Deployment Guide The 6NET Consortium. Viitattu 08.04.2014. http://www.6net.org/book/deployment-guide.pdf

Granlund, K. 2007. Tietoliikenne. Porvoo: WSOY

Jaakohuhta, H. 2005. Lähiverkot – Ethernet. 4., uudistettu painos. Helsinki: IT Press.

Paananen, J. 2005. Tietotekniikan peruskirja. Jyväskylä: Docendo Finland Oy.

Perahia, E. Stacey, R. 2008. Next generation wireless LANs. Cambridge: Cambridge university press.

Perlmutter, B. 2001. VPN - Virtuaaliset yksityisverkot. Helsinki: IT Press

Puska, M. 2000. Lähiverkkojen tekniikka. Jyväskylä: Gummerus Kirjapaino Oy

Puska, M 2005. Langattomat lähiverkot. Jyväskylä: Gummerus Kirjapaino Oy

Salo I. 2010. Cloud computing, palvelut verkossa. Jyväskylä: WSOY – Docendo.

Teknologiateollisuus 2010. Digitaalinen Suomi 2020. Teknologiateollisuus ry

Teletekno 2006. Optiset liityntäverkot. Teletekno Oy

VERKKOLÄHTEET:

Cisco 2013. Network Address Translation (NAT) FAQ. Viitattu 24.03.2014 http://www.cisco.com/c/en/us/support/docs/ip/network-address-translation-nat/26704-nat-faq-00.html

Cisco 2014. SSL VPN. Viitattu 11.04.2014 http://www.cisco.com/c/en/us/td/docs/ios/12_4t/12_4t11/htwebvpn.html

IEEE802. 2013. ISO/IEC TR 11801-99-1Guidance on 40GBASE-T Cabling. Viitattu 08.04.2014 http://www.ieee802.org/3/bq/public/may13/flatman_01_0513_40GBT.pdf

IPv6 ominaisuudet ja käyttöönotto. Viitattu 07.04.2014 http://ipv6.willab.fi/presentations/IPv6-esitelma.pdf

Eduskunta 2008. Paratiisi vai panoptikon – Näkökulmia uniikkiyhteiskuntaan. Viitattu 14.04.2014
http://lib.eduskunta.fi/dman/Document.phx?documentId=dz11508114736413&cmd=download

Sonkki, M 2013. Wideband and Multi-element Antennas for Mobile Applications, University of Oulu, The Department of Communications Engineering, PhD Thesis. Viitattu: 10.04.2014

Standards.ieee. 2014. NEW IEEE 802.11ac™ SPECIFICATION DRIVEN BY EVOLVING MARKET NEED FOR HIGHER, MULTI-USER THROUGHPUT IN WIRELESLANS. Viitattu: 08.04.2014
http://standards.ieee.org/news/2014/ieee_802_11ac_ballot.html

Tlu.ee .2014. Parikaapeleiden siirtokyky. Viitattu 11.03.2014
http://www.tlu.ee/~matsak/telecom/lasse/twisted_pair_cables/parikaapeleiden_siirtokykyvaatimukset.html

Liite 1

Porttitiedot

Cisco 887 VA-M

| | |
|---|---|
| Portti: Fe0/0 | Kohde: Zyxel Zywall 2Plus Wan 10/100M |

Zyxel Zywall 2Plus

| | |
|---|---|
| Portti: Lan1 | Kohde: AT-FS705LE Lan5 |
| Portti: Lan2 | Kohde: Buffalo NAS |
| Portti: Lan3 | Kohde: Rasia 8 (PC) |
| Portti: Lan4 | Kohde: Rasia 7 (PC) |

AT-FS705LE

| | |
|---|---|
| Portti: Lan1 | Kohde: Rasia 6 (PC) |
| Portti: Lan2 | Kohde: Rasia 4 (Printteri) |